AIRBUS

[Airbus Amber]

AIRBUS SECURITY REQUIREMENTS FOR SUPPLIERS

Dear Suppliers,

Cyber Security is one of AIRBUS' Top Priorities.

In this context, please be advised that the Directive A1015 is now attached to each PO and it is the supplier's responsibility to take note of the instructions therein.

A1015 defines Airbus' objectives and minimum requirements for Suppliers of goods and Services in terms of security and information risk management. This directive is set to explain the risks and threats faced by suppliers. In return, Airbus expects its suppliers to abide by the requirements intended to improve the overall level of protection and cyber resilience of our ecosystem.

Table of contents

Requirements on Information Security for Suppliers

PURPOSE/SCOPE:

This Directive defines the Airbus Security and Information Risk Management requirements for Suppliers. The purpose of this directive A1015.0 (hereafter the "Directive") is to maintain the security of Airbus business information, organizational information processing systems, products and facilities that are accessed, operated or processed by Suppliers and their own suppliers, located either on or off Airbus sites.

Airbus Procurement shall apply the Airbus Information Security Requirements as laid down in this Directive, without any deviation, to all Supplier Contracts/contractual arrangements with any Airbus entities, sites, locations including subsidiaries and Joint-Ventures in which Airbus has controlling interests. This Directive may be complemented by specific security specifications relevant for the contracted work or procured product if required by the sensitivity of information/connectivity or by applicable internal or external regulations.

Document Owner:

Name: KNUEPPEL Dietrich
Function: Directive Owner

Authorizer for Application:

Name: ANDREI Pascal
Function: SEC FoR Owner

Electronically validated - Released on 17 Jan 2018

TABLE OF CONTENTS

1 Introduction

There is a growing business demand to provide Airbus Suppliers with direct or integrated access to Airbus Information and Information Systems and consequently its Data, but it is recognized that this exposes Airbus to a variety of risks. The aim of this Directive is to define how the Suppliers are required to work in order to build up a trustworthy collaboration.

Airbus recognizes that by providing Suppliers with access to Information and Information Systems, risks are introduced through:

- loss of control where Airbus Information and Information Systems are accessed or operated by Suppliers,
- loss of control and responsibility where Airbus Information and Information Systems are located off Airbus sites,
- loss of visibility of Supplier activity related to Airbus security constraints.

It is also recognized that inappropriate protection of the Suppliers' own data and systems endangers both quality and in-time delivery of goods or services to Airbus. Therefore, adequate IT, OT or IoT security and business continuity on the Supplier side is also a requirement from an industrial point of view.

Therefore the requirements stated in this Directive shall be implemented in each of the following use cases:

- the Supplier accesses Airbus Information Systems, Airbus manufacturing systems (OT) or Airbus products by IT means (remotely or on site),
- the Supplier hosts Airbus Information,
- the Supplier leverages its own IT, OT or IoT systems to manufacture, deliver, install, maintain products, or provide services to Airbus.

In addition, the security of data in collaborative projects as well as internal information and data exchange is under increasing scrutiny by government agencies in Europe and the USA.

Cyber espionage also represents a substantial, and growing, threat to companies operating within certain key industries, including aerospace & defence technology. Well-developed cyber defences in Airbus provide a degree of security, but threats may also emanate from within the supply chain. Suppliers have access to Airbus Information and systems but may lack the requisite security infrastructure to adequately protect the information assets, and subsequently risk a passive breach of the agreed Non-Disclosure Agreement(s).

Airbus is committed to reflect the corresponding requirements by ensuring an appropriate level of information security in its supply chain.

2 Requirements

2.1 Requirements - Agreement on Collaborative Working

Airbus aims to co-operate with Suppliers according to mutually observed rules/agreements.

This document is applicable in complement of the "General Terms and Conditions (GTC) for Access to and Use of Airbus Supplier Portals".

Reference	***Designation***	***Applicability Condition***	***Origin***
ABR.SEC.A1015.0.1 - 2	The Supplier shall undertake to work professionally and to apply the security requirements contained herein in good faith.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.1.2; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.2 - 1	The Supplier shall be responsible for its day-to-day operational activities on Airbus systems and information, in accordance with this Directive.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.1.2; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.3 - 1	The Supplier shall implement a baseline protection in accordance with this Directive, prior to or upon performance of the Contract/contractual arrangements with Airbus.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.1.2; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.4 - 2	The Supplier shall be responsible for implementing appropriate general Security Risk Management processes and ensuring that its own subcontractors/suppliers also implements such Security Risk Management processes within their organizations. *Note 1: The Supplier re-assesses its Security Risks for Airbus on a regular basis since new vulnerabilities may be discovered, the threat landscape may evolve, organizations may change, and technology may progress.* *Note 2: The Supplier maintains a Security Risk register and treatment plan (accept, mitigate, avoid or transfer and notify Airbus of security risks that may affect the delivered services or goods.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.5 - 2	The Supplier shall only access, use, modify, and/or remove any aspects of Airbus system(s) or data as authorized by Airbus. *Note: The Supplier does not attempt to access any systems or information that has not been authorized by Airbus for contract execution.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.6 - 1	The Supplier shall not attempt to circumvent, modify or disable any of Airbus' network and/or systems security mechanisms.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.1.2
ABR.SEC.A1015.0.7 - 2	The Supplier shall be responsible for ensuring that no applicable Airbus security provisions (e.g. Acceptable Use Policy/ICT Charter when working in Airbus systems, Plant Regulations for visitors, on-site staff, etc.) are contravened unless written agreement has been reached with Airbus Security. *Note: The Supplier may require governmental accreditation (Facility Security Clearance) for work on some Airbus sites or projects.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.11.1.5
ABR.SEC.A1015.0.97 - 1	The Supplier shall protect from loss, destruction, falsification, corruption, unauthorized access and unauthorized release all relevant Airbus Information that it accesses, operates or processes. *Note: This protection continues even after the end of the contract.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus internal

2.2 Requirements - Initial Assessment

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.8 - 2	Prior to establishing any data exchange or any systems or networks connectivity, the Supplier shall provide to Airbus Security all required information and documentation to allow an assessment of Supplier's security level with regard to this Directive. *Note 1: This should include a copy of Supplier's current information security policy, including its policy regarding physical security for access to locations or devices that may connect to Airbus systems or process Airbus Information.* *Note 2: Airbus ensures confidentiality of all information provided by the Supplier.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.1.1

2.3 Requirements - Security Policies

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.10 - 1	The Supplier shall ensure formal management commitment and efficient user awareness, by developing and distributing a comprehensive, approved information security policy and user guidelines to all individuals with access to the Supplier's information and systems.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.5.1.1
ABR.SEC.A1015.0.11 - 1	Based on its information security policy, the Supplier shall establish a comprehensive set of operating standards and procedures aimed at privileged users (e.g. administrators, programmers) to ensure consistent implementation of information security controls.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.5.1.1

2.4 Requirements - Organization of Security

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.12 - 2	Appointment of Security Manager - the Supplier shall nominate one of its employees with overall accountability for security and risk issues and provide appropriate authority and means to this function to co-ordinate the activity across the organization.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.6.1.1
ABR.SEC.A1015.0.13 - 1	This Supplier's Security Manager shall be aware of all applicable statutory and contractual requirements, including but not limited to those laid down in this Directive and export compliance, affecting the Supplier's security controls, processes and systems.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.18.1.1
ABR.SEC.A1015.0.14 - 2	The Supplier shall nominate to Airbus Security a point of contact in its organization, and a back-up, who is responsible for routine collaboration and incident reporting.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.15 - 2	The Supplier shall segregate duties and areas of responsibility in the areas of security and IT, OT or IoT to reduce the risk of accidental or deliberate system or application misuse.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.6.1.2

2.5 Requirements - Human Resources Security

Reference	***Designation***	***Applicability Condition***	***Origin***
ABR.SEC.A1015.0.16 - 2	Solely the Supplier shall be responsible for the enforcement of Airbus security requirements within its organization and therefore ensures that the users are qualified and properly trained.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.17 - 2	The Supplier shall have in place systematic staff vetting processes for checking identity and background of its personnel. *Note 1: This should include verification of the highest obtained diploma, address of residence in recent years, references of previous employment, checking the validity of identity documents presented and the absence of any serious criminal offence.* *Note 2: In countries where such a process is restricted by laws and regulations, then the Supplier carry out the vetting process to the full extent permitted by the laws and regulations.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.18 - 1	The Supplier shall provide upon request security vetting information regarding its staff. *Note: For work subject to government regulations or other confidential projects, Airbus reserves the right to request security vetting information, if appropriate and to the extent permitted by law.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.19 - 1	The Supplier shall ensure that all employees and suppliers/subcontractors who have access to Airbus Information and data are made aware of the confidential nature of those information and of the obligations contained in this Directive, through appropriate training and awareness activities.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.2.2
ABR.SEC.A1015.0.20 - 2	The Supplier shall ensure that contracts with its employees and suppliers/ subcontractors comply with the confidentiality commitments contained in this Directive.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.1.2
ABR.SEC.A1015.0.21 - 2	The Supplier shall appoint staff responsible for management and security of its information systems, and shall notify Airbus without any delay of any change in such personnel. *Note: The Supplier undertakes that any replacement staff has an equivalent level of competence.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.22 - 1	In case a security issue related to a Supplier's employee is identified, Airbus may notify the Supplier of its disapproval regarding the allocation of this employee relating to Airbus work. In this case, the Supplier shall take all necessary steps to ensure that this employee is not given access to proprietary or confidential assets provided to the Supplier in relation with its work for Airbus. *Note: Assets mentioned above include but are not limited to information, documents and data, any information system (hardware and software), or physical products.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.7.2.3

2.6 Requirements - Asset Management

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.23 - 2	The Supplier shall consider Information being transferred between the Supplier and Airbus as classified "Airbus internal" (see A1044 - Protection and Classification of Information Directive) and secure it accordingly. *Note: Access to any classified information of higher levels is subject to a specific agreement.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.13.2.2; ISO 27001-2013-A.8.2.1; ISO 27001-2013-A.8.2.2
ABR.SEC.A1015.0.24 - 1	The Supplier shall implement information handling procedures in respect to Airbus classification levels (see A1044 - Protection and Classification of Information Directive), promote awareness and ensure compliance among its users.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.2.3
ABR.SEC.A1015.0.25 - 2	The Supplier shall maintain an up to date list of authorized IT, OT or IoT equipment that is used to access, transfer, process and/or store Airbus Information.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.26 - 1	Upon request, the Supplier shall provide Airbus with a list of all the systems and devices where Airbus Information is stored or processed (i.e. physical location, network location and business purpose of storing/processing).	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.27 - 1	In case the Supplier is ISO27001 certified, he shall add Airbus Information and connectivity with Airbus to the inventory of ISMS assets.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.1.1

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.28 - 2	The Supplier shall not store Airbus information on mobile devices (Smartphone's, laptops, USB drives, etc.) unless encrypted by state-of-the-art products/standards.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.1.3
ABR.SEC.A1015.0.29 - 1	Any used or broken storage media containing Airbus Information shall be effectively wiped or destroyed prior to being decommissioned or reused.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.3.2

2.7 Requirements - Access Control

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.30 - 2	The Supplier shall only use permitted access methods and controls as provided or required by Airbus.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.1.1
ABR.SEC.A1015.0.31 - 1	The Supplier shall duly identify and record the connections with Airbus networks and systems.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.32 - 1	The Supplier shall maintain a logical network diagram that includes external connections and specifically details the connection to Airbus.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.33 - 2	The Supplier shall maintain an up to date list of user authorizations on systems of its organization.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.34 - 2	The Supplier shall ensure the user request and authorization process for access rights to its own systems and to Airbus systems is traceable in its organization and complies with the need-to-know principle.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.35 - 1	The Supplier shall revoke, without any delay, access rights of any Supplier’s user who no longer requires access to Airbus systems and/or information for professional or contractual reasons.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.36 - 1	The Supplier shall notify Airbus immediately concerning any user access right revocations when there is a need for administrative actions by Airbus.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.1

Reference	***Designation***	***Applicability Condition***	***Origin***
ABR.SEC.A1015.0.37 - 3	The Supplier shall certify at least yearly that its users of Airbus IT, OT or IoT systems are legitimate and authorized as contractually stipulated. *Note: The supplier discloses the list of system users to the Airbus business owner of the contract or work package.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.5
ABR.SEC.A1015.0.38 - 3	The Supplier shall ensure that system and network accesses are logged and logs are retained for at least 12 months. *Note 1: The Supplier takes appropriate measures to ensure that transactions cannot be repudiated.* *Note 2: In countries where log retention is restricted by laws and regulations to less than 12 months, then the Supplier retains log data to the full extent permitted by the laws and regulations.* *Note 3: The log includes also creation/ change/revocation of access rights and user credentials.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.4.1
ABR.SEC.A1015.0.39 - 1	The Supplier shall ensure that users with elevated access rights (e.g. administrators) are monitored for abnormal activities, in addition to the logging of their system and network accesses and privilege use.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.4.1; ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.40 - 2	The Supplier shall ensure that the systems on which Airbus data is stored or processed, or from which Airbus systems are accessed, are protected against unauthorized accesses. *Note: Adequate security mechanisms are required on all layers such as network (including but not limited to adequately deployed and configured firewalls at the perimeter, restricted Internet and wireless access, customer/supplier connections, VPN remote access), operating systems and applications (including authentication and user management).*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.1.2; ISO 27001-2013-A.9.4.1; ISO 27001-2013-A.13.1.3

Reference	***Designation***	***Applicability Condition***	***Origin***
ABR.SEC.A1015.0.41 - 2	The Supplier shall ensure that all users of the network and computing devices have unique personal userIDs. *Note 1: This also includes administrator accounts. There must be no shared/group IDs in use, thus ensuring the confidentiality of systems and information as well as accountability of activity by users on the network.* *Note 2: Service accounts used by system processes and for machine-to-machine communications have a clear owner and be managed securely e.g. by restricting interactive logon, high password complexity and expiration rules.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.42 - 2	The Supplier shall ensure that Administrators have separate accounts for high privilege activities and normal usage (IT, OT or IoT) work (incl. Internet and e-mail use) not requiring elevated privileges to prevent malicious code be downloaded and executed under the high privileges. *Note: The non-privileged accounts are configured according to "least privileges" principle as for any other normal Supplier's user.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.43 - 2	The Supplier shall ensure that all access to its systems and information are controlled by the use of strong passwords and corresponding userIDs (in respect of the state of the art). *Note: These can be substituted by personalized digital certificates complying with agreed international standards.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.44 - 2	The Supplier shall isolate Airbus Information from its own information and other customers' information so that only authorized staff can access Airbus Information. *Note: The Supplier does not use the same physical working areas, IT, OT or IoT systems or application installations for Airbus and Airbus' competitors without consulting Airbus Security department.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.45 - 1	The Supplier shall not provide access to Airbus Information or systems to any other entity without prior written approval from Airbus.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal

2.8 Requirements - Cryptography

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.46 - 2	The Supplier shall use cryptographic tools (e.g. encryption, digital signature) compatible with the standards used by Airbus (interoperability) to ensure confidentiality and integrity and non-repudiation of data being transferred and/or stored, upon Airbus' request.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.10.1.1
ABR.SEC.A1015.0.47 - 1	For projects/programs subject to defence, governmental, NATO or OCCAR classification, the Supplier shall use the same cryptographic tools as Airbus for compliance and interoperability reasons. *Note: Airbus may be obliged to use specific cryptographic tools in the frame of certain programmes/projects if requested by the customer or authorities.*	Supplier - Supplier for Airbus of any kind of goods or services, subject to defense, governmental, NATO or OCCAR classification	Airbus Internal
ABR.SEC.A1015.0.48 - 2	Where applicable law restricts the use of cryptography, the Supplier shall assess and agree with Airbus alternative appropriate information protection mechanisms on a case-by-case basis.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.18.1.5

2.9 Requirements - Physical and Environmental Security

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.49 - 2	The Supplier shall ensure that access to its buildings, offices and computing facilities is controlled and limited (e.g. by use of locked doors, swipe card readers, burglary prevention, detection and response, etc.) in order to efficiently protect the confidentiality of information and access to critical systems and assets, and to prevent theft of documents or equipment.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.11.1.1
ABR.SEC.A1015.0.50 - 2	The Supplier shall further restrict access to certain specific areas: – areas hosting IT, OT or IoT infrastructure like server or network rooms, – areas where users with elevated access privileges are working, – areas with an elevated confidentiality level for Airbus (subject to specific agreement).	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.11.1.1

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.51 - 2	The Supplier shall ensure that business-critical IT, OT or IoT equipment is installed in a location where environmental risks (e.g. through earthquakes, flooding, extreme weather conditions) are reduced, and appropriate environmental controls are deployed to mitigate any potential physical damage (e.g. racks/cages, cable ducts, cooling system, Uninterruptible Power Supply (UPS), water detection, fire detection/suppression, hazardous material management etc.).	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.11.1.4; ISO 27001-2013-A.11.2.1
ABR.SEC.A1015.0.100 - 1	The Supplier shall implement a clean desk policy for papers and removable storage media and a clear screen policy for information processing facilities related to Airbus work.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus internal

2.10 Requirements - Operations Security

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.52 - 2	The Supplier shall ensure that formal change control procedures are established within the Supplier to ensure all changes performed on IT, OT or IoT systems and infrastructure (e.g. configurations, upgrades, new applications/components, etc.) are duly documented, tested and approved by the Supplier's IT, OT or IoT and/or business management.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.1.2; ISO 27001-2013-A.12.1.4
ABR.SEC.A1015.0.53 - 1	Except as provided for elsewhere under the contract between Airbus and the Supplier, the Supplier shall obtain specific agreement from Airbus Security department before processing any change that involves Airbus systems or data where the areas of Confidentiality, Availability, Integrity and Accountability may be affected.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.54 - 1	The Supplier shall perform regular backups of data and software and respect the following principles: – Store backups away from live systems, – Physically protect storage of backups with at least the same level as the live systems, – Regularly test restoration of backups.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.3.1
ABR.SEC.A1015.0.55 - 2	The Supplier shall ensure that key IT, OT or IoT equipment is covered by a manufacturer's warranty, or support within the organization, thus ensuring availability of systems and information.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.11.2.4

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.56 - 2	The Supplier shall use all care and means available, including any state of the art technology necessary, to prevent intrusion of malicious codes on all its IT, OT or IoT equipment, storage media and all possible infrastructure (e.g. servers, e-mail gateways, etc.), in order to prevent data corruption or loss of service.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.57 - 1	The Supplier shall ensure that patterns/ signatures of anti-intrusion and/or anti-virus mechanisms are updated regularly on all devices, including mobile ones.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.58 - 1	The Supplier shall ensure that critical patches are applied to systems as recommended by software vendors, and after being tested by the Supplier for compatibility with its installations.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.12.6.1
ABR.SEC.A1015.0.59 - 1	The Supplier shall implement appropriate Data Loss Prevention mechanisms to prevent unauthorized disclosure of Airbus Information.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal

2.11 Requirements - Communications Security

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.60 - 1	The Supplier shall comply with Airbus data exchange and connectivity standards and procedures, unless agreed otherwise in writing by Airbus.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.13.2.1
ABR.SEC.A1015.0.61 - 1	Should Airbus data be transferred through data networks which are not under the direct control of the Supplier (e.g. leased lines, the Internet), the Supplier shall take all adequate actions to ensure both the confidentiality and the integrity of the data in transit.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.13.2.2; ISO 27001-2013-A.13.1.1

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.62 - 2	The Supplier shall ensure that data traffic from and to the Internet or other untrusted networks (e.g. test environments, partners networks) is limited using robust security mechanisms and monitored for abnormal behavior, e.g. using proxies and gateways. *Note 1: Internet addresses known to be a risk for misuse or source of attacks are blocked. The same applies for potentially dangerous e-mails like spam, phishing and suspicious attachments.* *Note 2: The Supplier also prevents users bypassing those control mechanisms (e.g. users tunneling to alternative proxies, using webmail or personal cloud services to share business data or to download unauthorized material).*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.13.2.3
ABR.SEC.A1015.0.63 - 2	The Supplier shall only use equipment that has been approved by Airbus to connect to Airbus networks, systems or Airbus products (except "Supplier Portals"). *Note: Equipment on Airbus network are able to be monitored and patched (incl. anti-malware updates) by Airbus. Supplier's own equipment not meeting this requirement can only be connected on networks isolated from Airbus.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.13.1.3

2.12 Requirements - System Acquisition, Development and Maintenance

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.64 - 2	The Supplier shall ensure that its products delivered to Airbus and that contain IT, OT or IoT components (this includes but is not limited to software applications, manufacturing equipment with embedded computing facilities, industrial control and building management systems), are developed using a structured and approved system development methodology that ensures information security requirements are considered as part of the process, and consequently defined, documented, met by using secure coding rules and verified in the testing & acceptance phase.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.14.2.1

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.65 - 2	If required to be installed on or connected to Airbus IT, OT or IoT environment, the Supplier shall ensure that its products delivered to Airbus are able to be integrated in Airbus network security processes like anti-malware protection, vulnerability management, patching, access control, incident monitoring and logging. *Note: Products delivered by the Supplier to Airbus that contain IT, OT or IoT components include but is not limited to software applications, manufacturing equipment with embedded computing facilities, industrial control and building management systems.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.66 - 2	The Supplier shall ensure that its Supplier's remote maintenance and support of products delivered to Airbus is compliant with Airbus remote connection standards. *Note: Products delivered by the Supplier to Airbus that contain IT, OT or IoT components include but is not limited to software applications, manufacturing equipment with embedded computing facilities, industrial control and building management systems.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.9.1.2
ABR.SEC.A1015.0.99 - 1	Where the Supplier needs to connect its own IT, OT or IoT equipment to any of its own products in Airbus manufacturing or built into any Airbus product (aircraft, helicopters, satellites, drones, etc.) for configuration, software/data loading, testing or troubleshooting in Airbus manufacturing, delivery or maintenance environments, the Supplier shall ensure that this IT, OT or IoT equipment and the software therein: – are dedicated and restricted to this kind of activity and their use is subject to formal procedures, – are not connected to any other network than the product-internal one during operation at the Airbus product, – are authentic, intact/faultless and free of malware, this also includes any removable media connected to the equipment.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus internal

2.13 Requirements - Supplier Relationships

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.67 - 2	Should there be a need for the Supplier to give access to Airbus Information to one of its suppliers and/or subcontractors, the Supplier shall notify Airbus and shall cascade all requirements herein to the lower tier supplier and/or subcontractor by means of a specific agreement. *Note 1: The Supplier is solely accountable for the enforcement of Airbus security requirements within its own supply chain.* *Note 2: Beside industrial activities, this requirement also covers the Suppliers' IT, OT or IoT outsourcing/cloud providers and facility management and alike services with access to Airbus Information.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.68 - 2	The Supplier shall provide the agreement regarding security requirements between the Supplier and a lower tier supplier and/or subcontractor to Airbus upon request. *Note: Such an agreement does in no way establish a direct contractual relationship between Airbus and the Supplier's suppliers and/or subcontractor.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.69 - 2	The Supplier shall perform security and risk reviews in order to check the compliance of its subcontractor with this Directive. *Note 1: The Supplier is also responsible for reporting non-compliance findings to Airbus Security department.* *Note 2: Airbus reserves the right to further assess Supplier's suppliers and/or subcontractors with regards to this Directive, this assessment may be done by Airbus Security or an agreed independent auditor.* *Note 3: The Supplier is authorized to appoint an agreed independent auditor for this task.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.2.1
ABR.SEC.A1015.0.70 - 2	Under no circumstance shall the Supplier grant access to Airbus data or systems (including but not limited to routing or relaying) to any of its suppliers and/or subcontractors without Airbus' prior written authorization.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal

2.14 Requirements - Information Security Incident Management

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.71 - 1	The Supplier shall perform continuous monitoring of systems and networks, employ intrusion detection and prevention systems and record security events.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.72 - 1	The Supplier shall have appropriate controls in place to identify and counter sophisticated cyber-attacks like Advanced Persistent Threats (APT) and Command & Control channels.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.73 - 2	The Supplier shall implement a comprehensive and approved incident management process for information and systems that includes identification, response, recovery, reporting, evidence protection and post-implementation review of information security incidents. *Note: Incidents include but are not limited to: lost or stolen equipment, malfunctions, loss of power, overloads, mistakes by users/IT, OT or IoT staff, access violations, malware and hacking.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.16.1.1
ABR.SEC.A1015.0.74 - 2	The Supplier shall identify and resolve security weaknesses and incidents, minimize their business impacts and reduce the risk of similar incidents occurrence.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.16.1.1
ABR.SEC.A1015.0.75 - 2	Should security incidents occur that potentially affect Airbus systems or Information, the Supplier shall investigate and report the incident to Airbus Security without any delay even without request. *Note: Such incidents include but are not limited to: theft of equipment storing Airbus Information, leakage of Airbus data from Supplier's systems, compromise of systems connected to Airbus.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.2.1; ISO 27001-2013-A.16.1.2
ABR.SEC.A1015.0.76 - 2	The Supplier shall take any action to remedy detected or notified security incidents. *Note: Should Airbus detect in its systems any kind of security incident originating from the Supplier, Airbus notifies the Supplier immediately and reserves the right to temporarily discontinue or restrict the connectivity with the Supplier.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.16.1.5

2.15 Requirements - Information Security Aspects of Business Continuity Management

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.77 - 2	The Supplier shall have prepared a Business Continuity Programme for maintaining/restoring IT, OT or IoT services in the event of a major failure or of any kind of force majeure (including but not limited to: physical damage, power cuts, fire, natural disaster). *Note: Such a programme consists of Management Framework, Business Continuity Plans, Maintenance, Review & Testing and Business Resumption & Disaster Recovery.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.17.1.1
ABR.SEC.A1015.0.78 - 1	Management Framework - The Supplier shall have appropriate mechanisms, processes, defined roles and responsibilities in place to ensure on-going business processes and avoid major disruptions. *Note: This should encompass Risk identification and assessment, mitigation strategies, maintaining availability of the services, processes and products of the business through awareness, reviews and testing.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.17.1.1
ABR.SEC.A1015.0.79 - 1	Business Continuity Plans - The Supplier shall document and train its employees on its business continuity plans to ensure that the business continues to function at an effective level in the event of a major incident.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.17.1.2
ABR.SEC.A1015.0.80 - 1	Maintenance, Review & Testing - The Supplier shall be able to demonstrate that there is a regular review, maintaining and testing of the plans through exercises.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.17.1.3
ABR.SEC.A1015.0.81 - 2	Business Resumption & Disaster Recovery - The Supplier shall produce a Disaster Recovery plan for its Airbus-related activity and internal dependent systems and processes. *Note: This covers the planning and detailed steps to be taken during and after an incident so that business operations can be resumed in a back to normal state.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.17.1.2

2.16 Requirements - Compliance

Both Airbus and the Supplier undertake to comply with all relevant statutory requirements (in particular where the access arrangement is international, and spans different jurisdictions). These will vary for each Supplier and should be subject to review on a case-by-case basis.

Special attention shall be paid to conflicts of law notably related to data protection/privacy, monitoring, data retention and cryptography.

The Supplier acknowledges that Airbus Security or an independent auditor designated by Airbus may audit security of Supplier's systems, processes and procedures where Airbus systems or Information may be placed or accessed from.

Airbus reserves the right, upon reasonable notice, to perform compliance and/or implementation audits at its discretion.

Airbus reserves the right to discontinue or restrict the connectivity or information access for the Supplier in case of audit access is denied, corrective actions are not implemented, or lack of collaboration in case of a major security incident.

In the case of a significant change in the Supplier's situation (including but not limited to mergers, acquisitions or other Corporate re-organizations) or in its business activities, Airbus reserves the right to reassess the Supplier's compliance with Airbus security requirements as necessary to protect information and infrastructure assets associated with Airbus.

Reference	***Designation***	***Applicability Condition***	***Origin***
ABR.SEC.A1015.0.82 - 1	The Supplier shall ensure a regular review and audit of its: – systems' technical robustness, – compliance with policy, – procedures for safeguarding systems and information.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.18.2.1
ABR.SEC.A1015.0.83 - 1	The Supplier shall comply with all applicable intellectual property/copyright laws and regulations, and obtain all necessary software licences.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.18.1.2
ABR.SEC.A1015.0.84 - 2	The Supplier shall grant Airbus (or an agreed independent auditor) access to buildings, documents, systems etc. for the purpose of inspecting and validating the security arrangements in line with this Directive and for information security risk mitigation. *Note: This access may also flow down into the Supplier's supply chain, where it is deemed that data exchange or systems connectivity is made to Airbus systems.*	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.2.1

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.85 - 1	The Supplier shall make all necessary arrangements to provide Airbus with appropriate information for a security assessment to be made, by Airbus or an agreed independent auditor.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.15.2.1
ABR.SEC.A1015.0.86 - 1	The Supplier shall take all appropriate remedial actions in respect of any defects identified by the audit.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.88 - 2	The Supplier shall be able to provide Airbus with proof that its organization meets applicable Export Laws and Regulations and that it keeps the traceability of this so that it can satisfy any control. *Note: Airbus may check at any moment the reliability of the Supplier's organization in respect of these requirements (physical and logical). This includes but is not limited to ensuring the identity and nationality(-ies) of users, information access approval and control (this will include a formal user accreditation process), control of information flow, and audit trails.*	Supplier - Supplier for Airbus of any kind of goods, technical data or services subject to export control laws and regulations	Airbus Internal
ABR.SEC.A1015.0.90 - 2	Where the contractual relation requires the Supplier's access to information subject to defense, governmental, NATO or OCCAR classification, the Supplier shall put in place all technical and organizational means to comply with the National Secrets Act of the country in which he executes the contract, according to the classification levels provided by Airbus in the specific Programme Security Instruction or Security Aspect Letter.	Supplier - Supplier for Airbus of any kind of goods, technical data or services, subject to defense, governmental, NATO or OCCAR classification	Airbus Internal
ABR.SEC.A1015.0.91 - 1	The Supplier shall provide information to and cooperate with Airbus in response to any subpoena, investigation or the like seeking Airbus Information and provide information and assistance to Airbus to seek certification and the like relative to its Information including Information in the possession of the Supplier.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.92 - 2	The Supplier shall promptly notify Airbus upon the receipt of any request requiring that Airbus Information be supplied to any other third party, including public administrations or authorities. *Note: The Supplier uses all legal means to contest such access requests unless approved by Airbus.*	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal

2.17 Requirements - Termination/Disengagement

Reference	Designation	Applicability Condition	Origin
ABR.SEC.A1015.0.93 - 1	At or before the time of Contract signing, the Supplier shall provide Airbus with a termination plan that addresses how Airbus Information will be returned to Airbus at the end of this agreement, including backup and archival information, and how all Airbus Information will be permanently removed from Supplier's equipment and facilities.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.94 - 1	The Supplier shall ensure the protection of Airbus Information and systems including continuation of service at the expiry of the Contract/contractual arrangements and in compliance with the provisions contained in the Contract/contractual arrangements.	Supplier - Supplier for Airbus of any kind of goods or services	Airbus Internal
ABR.SEC.A1015.0.95 - 1	The Supplier shall immediately notify Airbus when access to certain or all Airbus data or systems is no longer needed to fulfil its obligations under the Contract/contractual arrangements.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.96 - 1	Upon expiry of the term agreed for use of the information, or when the information is no longer required, the Supplier shall dispose of the information as agreed with Airbus and ensure that it cannot be retrieved.	Supplier - Supplier for Airbus of any kind of goods or services	ISO 27001-2013-A.8.1.4

3 Referenced Documents

The documents listed below have been used to create this Directive. However, they are not to be considered as being an integral part of the Contract/contractual agreement between Airbus and the Supplier based on this Directive, unless clearly stated and referenced in the respective requirement. Airbus will provide the reference documents to the Supplier on request.

Nota bene: Any ISO or ISF document shall be procured directly by the Supplier, Airbus cannot provide those documents for copyright reasons.

Doc. Reference	*Title*
A1044	Security Requirements for Classification & Protection of Information
GTC	General Terms and Conditions for Access to and Use of Airbus Supplier Portals
ICT/IST Charter	Airbus Information Managements - Use of IST Facilities
ISO/IEC 27001	Information technology - Information security management systems - Requirements
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security controls
ISO/IEC 27003	Information technology - Security techniques - Information security
ISO/IEC 27036	Information technology - Security techniques - Information security for supplier relationships management system implementation guidance
IEC 62443 Part 2-1 2010	Industrial communication networks - Network and system security - Establishing an industrial automation and control system security program
SoGP April 2016	The ISF Standard of Good Practice for Information Security

4 Glossary

Always refer to LEXINET

Airbus	Means Airbus S.A.S. and its subsidiaries, affiliates, joint ventures and associated companies
Airbus Information	In the context of this Directive means Airbus' intellectual property rights, methods, know-how, proprietary and/or privileged technology and processes, internal facts and figures, and any related material and document. This comprises all possible means and methods of storage and transmission in any format and on any media (including but not limited to paper documents, printouts, microfiche, electronic data in any form, pictures, and multimedia)
Airbus Security	Means in the context of this Directive the organization and people in Airbus responsible to protect Airbus staff, information, activities, scientific and technological heritage, assets and reputation, against all hostile acts, in such a way as to prevent, detect and respond to such hostile acts
Business Continuity	In the context of this Directive, this means the strategic and tactical capability of the Supplier's organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable level to ensure contract performance

Cyber	In the context of this Directive, this is the dynamic, always online, technologically interconnected world; it consists of people, organizations, information and technology. It is constantly changing in unpredictable ways, facilitates collaboration but de-risks criminal activity, concentrates targets and hides the perpetrators
Data	In the context of this Directive, this means all information in electronic form in any format and on any media
Information Security	Means safeguarding of: – Availability - to prevent loss of information and services, e.g. from malicious code, natural disasters, system failures/malfunctions – Integrity - to prevent unauthorised input, alteration, processing, deletion – Confidentiality - to prevent unauthorised disclosure – Accountability - to ensure identity of users and individual responsibility and audit trails for access and for transactions, to prevent and detect any fraudulent intrusion
Information Technology or IT	In the context of this Directive, this means any information technology or telecommunications equipment or services, any software, and associated processes, for storage, processing and transmitting of data. It namely includes PCs, workstations, laptops, removable media, phones, smartphone, networks, systems, computer programs, servers, databases and web portals
ISF	Information Security Forum
ISMS	Information Security Management System
NATO	North Atlantic Treaty Organization
OCCAR	Organisation Conjointe de Coopération en matière d'Armement
Operational Technology or OT	In the context of this Directive, this means any data management or communication technology or telecommunications equipment or services, any firmware, software, and associated processes, for storage, processing and transmitting of data embedded into manufacturing equipment (OT). It namely includes Human-to-Machine Interface, front end interface, removable media, networks, Programmable Logic Controllers (PLCs) used within manufacturing and building controls
Risk	In the context of this Directive, this means an event or condition that, should it occur, would have a negative impact on objectives and contract performance of the Supplier in terms of design, production and/or the future delivery of products/services to Airbus
Risk management	A forward-looking management process, which anticipates possible Risks to the Supplier's business objectives, and provides for their mitigation, so that Information Systems are not themselves exposed (or in turn affect the supported business processes) to consequences, which reasonably shall have been foreseen and avoided
Supplier	In the context of this Directive, this means those entities providing goods and/or services for Airbus' benefit and which are not part of Airbus (including but not limited to suppliers, subcontractors, service providers, industrial partners, and research centers)

The Internet of things or IoT	in the context of this Directive is the network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure

Contributors

Name	***Function***
ALTSTÄDT Kai	Prod. Indust & Operational Security MGR - EIDS
BALLARD Florence	Security Business Partners - ZSB
BOUDET Florent	Security Assurance - ZSG
DENIS Pierrette	Security Operations - ZSO
GAUVRY Philippe	Q Procurement Requirements Proj Mgr - QPR
JORDAN Marie	Prod. Secur capabilities Compliance MGR - EIDC1
MEIER-HEDDE Felix	Prod. Indust & Operational Security MGR - EIDS
REY Nathalie	Prod. Indust & Operational Security MGR - EIDS
THORNARY Mathieu	IM Security Analyst - ZIST
TREDEZ Juliette	Governance - ZSG
UTH Fridtjof	Security Assurance - ZSG

Record of Revisions

Issue	***Date***	***Reasons for Revision***
A	Dec 2017	Initial issue. Document completely reviewed. Merge of Airbus A1015 and former Airbus Group E260, incl. Airbus Helicopters and Airbus Defence&Space requirements, and product/OT aspects.

Electronically validated - Released on 17 Jan 2018

Requirements on Information Security for Suppliers
Validation Report

APPROVAL

Name [Siglum]	Date	
GAUVRY PHILIPPE [QPR]	18 Dec 2017	Electronically validated
CANCEILL VERONIQUE [PYD]	22 Dec 2017	Electronically validated
ALARY-TOSSAINT PHILIPPE [PYC]	11 Jan 2018	Electronically validated

AUTHORIZATION

Name [Siglum]	Date	
KNUEPPEL DIETRICH [ZSG]	12 Jan 2018	Electronically validated

AUTHORIZATION FOR APPLICATION

Name [Siglum]	Date	
ANDREI PASCAL [ZS]	17 Jan 2018	Electronically validated

Exigences Relatives à la Sécurité de l'Information pour les Fournisseurs

OBJET/DOMAINE D'APPLICATION :

La présente Directive définit les exigences d'Airbus relatives à la Gestion des Risques liés à l'Information et à la Sécurité destinées aux Fournisseurs. La présente directive A1015.0 (ci-après désignée "Directive") a pour objet de préserver la sécurité des informations commerciales, des installations, des produits et des systèmes de traitement des informations organisationnelles d'Airbus, consultées, exploitées ou traitées par les Fournisseurs et leurs propres fournisseurs, et dont les activités s'exercent sur des sites Airbus ou hors site.

Le Procurement d'Airbus doit appliquer les exigences en matière de sécurité de l'information d'Airbus mentionnées dans la présente Directive, sans écart d'aucune sorte, à tous les contrats ou dispositions contractuelles passés entre les Fournisseurs et tous les sites, entités et lieux d'implantation d'Airbus, y compris les filiales et joint-ventures au sein desquels Airbus a des intérêts majoritaires. La présente Directive peut être complétée par des spécifications de sécurité concernant spécifiquement les travaux sous-traités ou les produits achetés, si le caractère sensible des informations ou de la connectivité l'exige, ou par tout règlementation interne ou externe applicable.

Propriétaire du Document :

Nom : KNUEPPEL Dietrich

Fonction : Directive Owner

Autorisation pour Application :

Nom : ANDREI Pascal

Fonction : SEC FoR Owner

TABLE DES MATIERES

1 Introduction

Il existe une demande croissante pour fournir les fournisseurs d'Airbus avec des accès intégré ou direct aux Informations et Systèmes d'Information d'Airbus et, par conséquent, à ses données. Cette situation expose la Société à un grand nombre de risques. La présente Directive a pour but de définir la manière dont les Fournisseurs doivent collaborer pour établir des relations professionnelles basées sur la confiance.

Airbus reconnaît qu'en accordant à ses Fournisseurs un accès à ses informations et systèmes d'information, il favorise l'introduction de risques par :

- la perte de maîtrise dès lors que l'accès ou l'exploitation des informations et systèmes d'information d'Airbus s'effectue par les Fournisseurs ;
- la perte de maîtrise et de responsabilité dès lors que les informations et systèmes d'information d'Airbus se situent en dehors des sites Airbus ;
- la perte de visibilité de l'activité Fournisseur en matière de contraintes liées à la sécurité d'Airbus.

Une protection insuffisante des systèmes et données appartenant aux Fournisseurs compromet tant la qualité que la livraison, dans les délais prescrits, des biens ou services à Airbus. Ainsi, une sécurité des systèmes d'information (IT), de l'Internet des objets connectés (IoT) et de la technologie opérationnelle (OT) adéquate et une continuité opérationnelle côté Fournisseur constituent également une exigence d'un point de vue industriel.

Par conséquent, les exigences mentionnées dans la présente Directive doivent être mises en œuvre dans chacun des cas d'utilisation suivants :

- le Fournisseur accède aux systèmes d'information d'Airbus, aux systèmes de production d'Airbus (OT, technologie opérationnelle) ou aux produits d'Airbus via des moyens informatiques (à distance ou in situ),
- le Fournisseur héberge des informations d'Airbus,
- le Fournisseur exploite ses propres systèmes d'information (IT), technologie opérationnelle (OT) ou d'Internet des objets connectés (IoT) pour produire, livrer, installer, maintenir des produits, ou fournir des services à Airbus.

Par ailleurs, la sécurité des données dans le cadre de projets concertés ainsi que l'échange de données et d'informations internes sont soumis à un examen toujours plus minutieux de la part des organismes publics en Europe et aux Etats-Unis.

Le cyber-espionnage représente également une menace sérieuse qui ne cesse de s'accroitre pour les entreprises travaillant dans certains domaines clés, notamment l'aérospatial et la défense. Des cyber-défenses bien développées confèrent à Airbus un certain degré de sécurité, mais des menaces peuvent toujours provenir de l'intérieur de la chaîne d'approvisionnement. Les Fournisseurs ont accès aux systèmes et informations Airbus, mais les infrastructures de sécurité adéquates peuvent leur faire défaut pour protéger efficacement ces actifs, créant ainsi une violation passive des accords de confidentialités signés.

Airbus s'est engagé à refléter les exigences correspondantes en garantissant un niveau adéquat de sécurité de l'information au sein de sa chaîne d'approvisionnement.

2 Exigences

2.1 Exigences - Accord sur le Travail Collaboratif

Airbus se donne pour but de collaborer avec ses Fournisseurs conformément à des accords/ règles mutuellement respectés.

Ce document s'applique en complément du document "General Terms and Conditions (GTC) for Access to and Use of Airbus Supplier Portals" (Conditions générales d'accès et d'utilisation des portails Fournisseurs Airbus).

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.1 - 2	Le Fournisseur s'engage à travailler selon des méthodes professionnelles et à appliquer les exigences de sécurité spécifiées dans le présent document de bonne foi.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.1.2 ; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.2 - 1	Le Fournisseur est responsable de ses activités opérationnelles quotidiennes sur les systèmes et informations Airbus conformément à la présente Directive.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.1.2 ; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.3 - 1	Le Fournisseur doit mettre en œuvre une base minimale de protection, conforme à la présente Directive, avant ou au moment de l'exécution du Contrat/des dispositions contractuelles avec Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.1.2 ; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.4 - 2	Le Fournisseur est responsable de la mise en œuvre des processus appropriés de gestion des risques de sécurité généraux et de garantir que ses propres sous-traitants/fournisseurs mettent également en œuvre ces processus de gestion des risques de sécurité au sein de leurs propres organisations. *Nota 1 : Le Fournisseur réévalue périodiquement ses risques de sécurité pour Airbus dans la mesure où de nouvelles vulnérabilités peuvent être découvertes, le paysage des menaces évoluer, les organisations changer, et la technologie progresser.* *Nota 2 : Le Fournisseur maintient un registre des risques de sécurité et un plan de traitement (acceptation, atténuation, évitement ou transfert) et notifie Airbus des risques de sécurité pouvant impacter les services ou biens livrés.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.5 - 2	Le Fournisseur ne peut accéder, utiliser, modifier et/ou supprimer un aspect quelconque du ou des systèmes ou données d'Airbus que si Airbus l'autorise. *Nota : Le Fournisseur ne doit pas tenter d'accéder à l'un quelconque des systèmes ou informations dont l'accès n'est pas autorisé par Airbus dans le cadre de l'exécution du contrat.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.6 - 1	Le Fournisseur ne doit pas tenter de contourner, modifier ou désactiver l'un des mécanismes de sécurité des réseaux et/ou systèmes d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.1.2
ABR.SEC.A1015.0.7 - 2	Le Fournisseur a la responsabilité de s'assurer qu'aucune des dispositions de sécurité applicables d'Airbus (par ex. politiques d'Usage/ICT Charter en cas d'intervention sur des systèmes Airbus, Règlement Interieur destiné aux visiteurs, personnel in situ, etc...) n'est transgressée, sauf si un accord écrit a été conclu préalablement avec le Département Sécurité d'Airbus. *Nota : Le Fournisseur peut nécessiter un agrément gouvernemental (Habilitation pour les installations) pour pouvoir travailler sur certains sites ou projets d'Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.11.1.5
ABR.SEC.A1015.0.97 - 1	Le Fournisseur doit se protéger de la perte, de la destruction, de la falsification, de la corruption, de l'accès non autorisé et de la publication non autorisée de toutes les informations pertinentes d'Airbus auxquelles il a accès, qu'il exploite ou traite. *Nota : Cette protection continue même après la fin du contrat.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.2 Exigences - Evaluation Initiale

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.8 - 2	Avant de mettre en place tout échange de données ou connexion de systèmes ou de réseaux, le Fournisseur doit fournir au Département Sécurité d'Airbus toutes les informations et documentations requises pour permettre une évaluation du niveau de sécurité du Fournisseur en regard de la présente Directive. *Nota 1 : Cela doit inclure une copie de sa politique sur la sécurité de l'information en vigueur, notamment sa politique de sécurité physique pour l'accès aux sites ou appareils susceptibles de se connecter aux systèmes Airbus ou de traiter des informations Airbus.* *Nota 2 : Airbus veille à la confidentialité de toutes les informations fournies par le Fournisseur.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.1.1

2.3 Exigences - Politiques de Sécurité

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.10 - 1	Le Fournisseur doit garantir l'engagement formel de la direction et assurer une sensibilisation efficace auprès des utilisateurs en développant et diffusant une politique de sécurité de l'information exhaustive et approuvée et un guide utilisateur à toute personne ayant accès aux systèmes et informations du Fournisseur.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.5.1.1
ABR.SEC.A1015.0.11 - 1	Sur la base de sa politique de sécurité de l'information, le Fournisseur doit établir un ensemble exhaustif de normes et procédures de fonctionnement destiné à des utilisateurs dotés de privilèges (par exemple, administrateurs, programmeurs) afin de s'assurer de la bonne mise en œuvre des contrôles de sécurité de l'information.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.5.1.1

2.4 Exigences - Organisation de la Sécurité

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.12 - 2	Nomination du Security Manager - Le Fournisseur doit nommer l'un de ses employés, lequel aura la responsabilité globale des questions liées à la sécurité et aux risques. Cette personne sera investie de l'autorité nécessaire et aura les moyens appropriés pour coordonner les activités au sein de l'organisation.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.6.1.1
ABR.SEC.A1015.0.13 - 1	Le Security Manager du Fournisseur doit connaître toutes les exigences réglementaires et contractuelles applicables (y compris, à titre non limitatif, celles mentionnées dans la présente Directive et celles concernant la conformité à l'exportation) ayant un effet sur les contrôles, procédés et systèmes de sécurité du Fournisseur.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.18.1.1
ABR.SEC.A1015.0.14 - 2	Le Fournisseur doit nommer, au sein de son organisation, un point de contact pour le Département Sécurité d'Airbus, et un point de contact alternatif, qui sera responsable du reporting de routine et des incidents.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.15 - 2	Le Fournisseur doit séparer les tâches et domaines de responsabilités dans les domaines de la sécurité et des systèmes d'information, de l'Internet des objets connectés et de la technologie opérationnelle, afin de réduire le risque d'utilisation inappropriée intentionnelle ou accidentelle des systèmes ou applications.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.6.1.2

2.5 Exigences - Sécurité des Ressources Humaines

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.16 - 2	Seul le Fournisseur est responsable de la mise en application des exigences de sécurité Airbus au sein de son organisation et il s'assure donc que les utilisateurs sont qualifiés et ont reçu une formation adéquate.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.17 - 2	Le Fournisseur doit mettre en place des enquêtes de sécurité systématiques sur les membres du personnel, afin de vérifier leur identité et antécédents. *Nota 1 : Ces processus doivent inclure la vérification du diplôme le plus élevé obtenu, l'adresse personnelle des dernières années, les références d'emplois antérieurs, le contrôle de validité des pièces d'identité fournies et l'absence d'infraction criminelle grave au casier judiciaire.* *Nota 2 : Dans les pays où ce type de processus est réglementé, le Fournisseur met en place ce processus de vérification dans la limite autorisée par les lois et règlements nationaux.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.18 - 1	Sur demande, le Fournisseur doit transmettre les résultats des vérifications de sécurité portant sur son personnel. *Nota : Pour les travaux soumis à des règlements gouvernementaux ou autres projets confidentiels, Airbus se réserve le droit de demander des vérifications de sécurité, si besoin et dans les limites autorisées par la loi.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.19 - 1	Le Fournisseur doit veiller, par des activités de formation et de sensibilisation adéquates, à ce que tous les employés et fournisseurs/sous-traitants ayant accès aux données et informations Airbus soient sensibilisés au caractère confidentiel de ces informations et aux obligations spécifiées dans la présente Directive.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.2.2
ABR.SEC.A1015.0.20 - 2	Le Fournisseur doit s'assurer que les contrats passés avec ses employés et fournisseurs/sous-traitants respectent les engagements de confidentialité mentionnés dans la présente Directive.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.1.2

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.21 - 2	Le Fournisseur doit désigner des responsables de la sécurité et de la gestion de ses systèmes d'information parmi les membres du personnel et aviser immédiatement Airbus de tout changement affectant ce personnel. *Nota : Le Fournisseur s'engage à ce que tout membre désigné comme remplaçant possède un niveau de compétence équivalent.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.22 - 1	Si un problème de sécurité est détecté en rapport avec un employé du Fournisseur, Airbus a la possibilité de notifier le Fournisseur de sa désapprobation quant aux attributions de cet employé dans le cadre des travaux Airbus. Dans ce cas, le Fournisseur doit prendre toutes les mesures nécessaires pour s'assurer que cet employé n'ait pas accès aux actifs exclusifs ou confidentiels mis à la disposition du Fournisseur dans le cadre de son travail pour Airbus. *Nota : Les actifs mentionnés dans le point ci-dessus incluent, à titre non limitatif, les informations, documents, données, systèmes d'information (logiciel et matériel) ou produits physiques.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.7.2.3

2.6 Exigences - Gestion des Actifs

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.23 - 2	Le Fournisseur doit considérer les informations transmises entre le Fournisseur et Airbus comme étant classifié "Airbus internal" (voir Directive A1044 - Protection et Classification des Informations) et les protéger en conséquence. *Nota : L'accès à des informations classifiées de plus haut niveau fait l'objet d'un accord spécifique.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.13.2.2 ; ISO 27001-2013-A.8.2.1 ; ISO 27001-2013-A.8.2.2
ABR.SEC.A1015.0.24 - 1	Le Fournisseur doit mettre en œuvre des procédures de traitement des informations conformément aux niveaux de classification Airbus (voir Directive A1044 - Protection et Classification des Informations), promouvoir la sensibilisation à ces procédures et garantir leur respect par les utilisateurs.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.2.3

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.25 - 2	Le Fournisseur doit tenir à jour une liste de tous les équipements autorisés liés aux systèmes d'information, à l'Internet des objets connectés et à la technologie opérationnelle, utilisés pour l'accès, le transfert, le traitement et/ou le stockage des informations Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.26 - 1	Sur demande, le Fournisseur doit transmettre à Airbus la liste de tous les systèmes et supports de stockage et de traitement des informations Airbus (à savoir emplacement physique, emplacement réseau et objet du stockage/traitement).	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.27 - 1	Si le Fournisseur est certifié ISO 27001, il doit ajouter les connexions et informations Airbus à l'inventaire de ses systèmes de gestion de la sécurité de l'information.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.28 - 2	Le Fournisseur n'est pas autorisé à stocker des informations Airbus sur des appareils mobiles (smartphones, ordinateurs portables, clés USB, etc...), sauf si elles ont été cryptées à l'aide de produits ou de techniques de pointe.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.1.3
ABR.SEC.A1015.0.29 - 1	Tout support usé ou endommagé contenant des informations Airbus doit être formaté ou détruit de manière efficace avant d'être mis hors service ou réutilisé.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.3.2

2.7 Exigences - Contrôle de l'Accès

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.30 - 2	Le Fournisseur ne peut utiliser que les contrôles et les méthodes d'accès fournis ou exigés par Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.1.1
ABR.SEC.A1015.0.31 - 1	Le Fournisseur doit dûment identifier et enregistrer les connexions aux systèmes et réseaux d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.32 - 1	Le Fournisseur doit tenir à jour un schéma logique du réseau comprenant les connexions externes et détaillant spécifiquement les connexions au réseau Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

Référence	Description	Applicabilité	Origine
ABR.SEC.A1015.0.33 - 2	Le Fournisseur doit tenir à jour une liste de toutes les autorisations utilisateurs sur les systèmes de son organisation.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.34 - 2	Le Fournisseur doit assurer, au sein de son organisation, la traçabilité des demandes et attributions des droits d'accès utilisateurs à ses propres systèmes et aux systèmes Airbus selon le principe du "besoin d'en connaître".	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.35 - 1	Le Fournisseur doit révoquer sans délai, les droits d'accès de ses utilisateurs n'ayant plus besoin d'accéder aux systèmes et/ou informations Airbus pour des raisons professionnelles ou contractuelles.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.36 - 1	Le Fournisseur doit informer immédiatement Airbus de toute révocation de droits d'accès utilisateurs, dès lors qu'une action administrative de la part d'Airbus est nécessaire.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.37 - 3	Le Fournisseur doit certifier, au moins une fois par an, que les utilisateurs des systèmes d'information, de l'Internet des objets connectés et de la technologie opérationnelle d'Airbus ont toute légitimité et sont dûment autorisés, conformément aux clauses contractuelles. *Nota : Le Fournisseur transmet la liste des utilisateurs des systèmes au maître d'ouvrage Airbus pour le contrat ou lot de travaux (WP) en question.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.5
ABR.SEC.A1015.0.38 - 3	Le Fournisseur doit s'assurer que les accès aux systèmes et réseaux sont enregistrés et que les journaux sont conservés pendant au moins 12 mois. *Nota 1 : Le Fournisseur prend les mesures appropriées pour s'assurer que les transactions ne puissent être répudiées.* *Nota 2 : Dans les pays où la conservation de ces archives est limitée à moins de 12 mois, le Fournisseur les conserve dans la limite autorisée par les lois et règlements nationaux.* *Nota 3 : Le journal inclut également la création/modification/révocation des droits d'accès et des identifiants.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.4.1

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.39 - 1	Le Fournisseur doit s'assurer de la surveillance des utilisateurs possédant des droits d'accès de niveau élevé (par exemple, les administrateurs) pour vérifier l'absence de toute activité anormale, en plus de la journalisation de leurs accès aux systèmes et réseaux et de leur utilisation privilégiée.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.4.1 ; ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.40 - 2	Le Fournisseur doit s'assurer que les systèmes sur lesquels les données Airbus sont stockées ou traitées, ou à partir desquels les systèmes Airbus sont consultés, sont protégés contre les accès non autorisés. *Nota : Des mécanismes de sécurité adéquats doivent être mis en place sur toutes les couches telles que le réseau (y compris, à titre non limitatif, pare-feu correctement configurés et déployés en périphérie, restriction des accès internet et sans fil, des connexions client/fournisseur, des accès distants VPN), les systèmes d'exploitation et les applications (y compris la gestion des utilisateurs et l'authentification).*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.1.2 ; ISO 27001-2013-A.9.4.1 ; ISO 27001-2013-A.13.1.3
ABR.SEC.A1015.0.41 - 2	Le Fournisseur doit s'assurer que tous les utilisateurs du réseau et des dispositifs informatiques possèdent un code d'identification utilisateur personnel unique. *Nota 1 : Ceci concerne également les comptes administrateurs. Pour garantir la confidentialité des systèmes et des informations ainsi que l'imputabilité de l'activité aux utilisateurs sur le réseau, aucun code d'identification de groupe/ partagé n'est autorisé.* *Nota 2 : Les comptes de service utilisés par les processus système et pour les communications entre machines auront un propriétaire clairement défini et seront gérés de manière sécurisée, par exemple en limitant la connexion interactive, à l'aide de règles de mots de passe forts et d'expiration.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.1

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.42 - 2	Le Fournisseur doit s'assurer que les administrateurs possèdent des comptes séparés pour les activités nécessitant des droits d'accès de niveau élevé et un usage normal (systèmes d'information, technologie opérationnelle ou Internet des objets connectés) (y compris l'utilisation d'Internet et l'envoi d'e-mails ne nécessitant pas de privilèges élevés), afin d'éviter que des codes malveillants ne soient téléchargés et exécutés à leur niveau de privilèges élevé. *Nota : Les comptes sans niveau de privilèges élevé sont configurés selon le principe des "moindres privilèges" comme pour tout autre utilisateur normal du Fournisseur.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.43 - 2	Le Fournisseur doit s'assurer que tous les accès à ses systèmes et ses informations sont contrôlés par l'utilisation de mots de passe forts et des identifiants correspondants (conformément aux dernières technologies). *Nota : Ces derniers peuvent être remplacés par des certificats numériques personnalisés en conformité avec les standards internationaux convenus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.44 - 2	Le Fournisseur doit isoler les informations Airbus de ses propres informations et des informations des autres clients, afin que seul le personnel autorisé ait accès aux informations Airbus. *Nota : Le Fournisseur n'utilise pas les mêmes zones de travail physiques, systèmes d'information, technologie opérationnelle ou Internet des objets, ou installations d'applications pour Airbus et ses concurrents, sans consulter préalablement le Département Sécurité d'Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.45 - 1	Le Fournisseur ne doit pas permettre à une entité tierce d'accéder aux systèmes et informations Airbus sans l'autorisation écrite préalable d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.8 Exigences - Cryptographie

Référence	Description	Applicabilité	Origine
ABR.SEC.A1015.0.46 - 2	Le Fournisseur doit utiliser des outils cryptographiques (ex. : cryptage, signature numérique) compatibles avec les normes utilisées par Airbus (interopérabilité) pour garantir la confidentialité, l'intégrité et la non-répudiation des données transférées et/ou stockées, à la demande d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.10.1.1
ABR.SEC.A1015.0.47 - 1	Pour les projets ou programmes soumis à une classification défense, gouvernementale, OTAN ou OCCAR, le Fournisseur doit utiliser les mêmes outils cryptographiques qu'Airbus pour des raisons de conformité et d'interopérabilité. *Nota : Airbus peut être obligé d'utiliser des outils cryptographiques spécifiques dans le cadre de certains programmes et projets, si le client ou les autorités le demandent.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services soumis à une classification défense, gouvernemen-tale, OTAN ou OCCAR	Airbus internal
ABR.SEC.A1015.0.48 - 2	Lorsqu'une loi en vigueur restreint l'utilisation de la cryptographie, le Fournisseur doit évaluer et convenir avec Airbus des mécanismes appropriés de protection des informations au cas par cas.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.18.1.5

2.9 Exigences - Sécurité Physique et Environnementale

Référence	Description	Applicabilité	Origine
ABR.SEC.A1015.0.49 - 2	Le Fournisseur doit s'assurer que l'accès à ses bâtiments, bureaux et systèmes informatiques est contrôlé et limité (par exemple, par l'utilisation de portes verrouillées, de lecteurs de cartes magnétiques, la prévention du cambriolage, la détection et l'intervention, etc...) pour une protection efficace de la confidentialité des informations et de l'accès à des systèmes et équipements critiques, et une prévention des vols de documents et d'équipements.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.11.1.1

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.50 - 2	De plus, le Fournisseur doit restreindre l'accès à certaines zones spécifiques : – zones hébergeant des infrastructures liées aux systèmes d'information, technologie opérationnelle ou Internet des objets connectés comme les salles de serveurs ou de réseaux ; – zones où travaillent des utilisateurs possédant des droits d'accès de niveau élevé ; – zones ayant un niveau élevé de confidentialité pour Airbus (soumis à un accord spécifique).	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.11.1.1
ABR.SEC.A1015.0.51 - 2	Le Fournisseur doit s'assurer que les équipements liées aux systèmes d'information, technologie opérationnelle ou Internet des objets connectés critiques pour l'activité sont installés dans un emplacement où les risques environnementaux (par exemple, tremblements de terre, inondations, conditions météorologiques extrêmes) sont réduits, et des dispositifs appropriés de contrôle de l'environnement sont déployés pour réduire tout dommage matériel potentiel (par exemple, baies/cages, conduits de câbles, conditionnement d'air, alimentation secourue, détection d'eau, détection/extinction d'incendie, gestion des matières dangereuses, etc...).	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.11.1.4 ; ISO 27001-2013-A.11.2.1
ABR.SEC.A1015.0.100 - 1	Le Fournisseur doit mettre en œuvre une politique du "bureau vide" pour les documents papier et les supports de stockage amovibles ainsi qu'une politique de l'"écran vide" pour les installations de traitement des informations liées aux travaux d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.10 Exigences - Sécurité des Opérations

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.52 - 2	Le Fournisseur doit s'assurer que des procédures formelles de contrôle des modifications doivent être mises en place chez le Fournisseur pour garantir que toutes les modifications réalisées sur l'infrastructure et les systèmes d'information, technologie opérationnelle ou Internet des objets connectés (par exemple, configurations, mises à niveau, nouvelles applications/nouveaux composants, etc...) sont dûment documentées, vérifiées et approuvées par la direction des systèmes d'information, technologie opérationnelle ou Internet des objets connectés et/ou opérationnelle du Fournisseur.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.1.2 ; ISO 27001-2013-A.12.1.4
ABR.SEC.A1015.0.53 - 1	Sous réserve d'autres dispositions éventuelles au titre du contrat conclu entre Airbus et le Fournisseur, le Fournisseur doit obtenir un accord spécifique du Département Sécurité d'Airbus avant de procéder au traitement de toute modification s'appliquant à des systèmes ou données Airbus et susceptible d'avoir un impact dans les domaines suivants : confidentialité, disponibilité, intégrité et imputabilité.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.54 - 1	Le Fournisseur doit effectuer régulièrement des sauvegardes des données et des logiciels et respecter les principes suivants : – stocker les sauvegardes à distance des systèmes opérationnels ; – protéger physiquement les sauvegardes en appliquant au moins le même degré de protection que pour les systèmes opérationnels ; – tester périodiquement la restauration des sauvegardes.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.3.1
ABR.SEC.A1015.0.55 - 2	Le Fournisseur doit s'assurer que les équipements liés aux systèmes d'information, technologie opérationnelle ou Internet des objets connectés clés sont couverts par une garantie du fabricant, ou par un support au sein de l'organisation, afin d'assurer la disponibilité des systèmes et des informations.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.11.2.4

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.56 - 2	Le Fournisseur doit employer tous les moyens disponibles, et technologies de pointe nécessaires, pour éviter toute intrusion de codes malveillants sur les équipements, supports de stockage et toute l'infrastructure possible des systèmes d'information, technologie opérationnelle ou Internet des objets connectés (à savoir serveurs, passerelles de messagerie électronique, etc...) afin d'éviter l'altération de données et la perte de service.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.57 - 1	Le Fournisseur doit s'assurer que les modèles/signatures des mécanismes anti-intrusion et/ou anti-virus sont régulièrement actualisés sur tous les dispositifs, y compris les dispositifs mobiles.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.58 - 1	Le Fournisseur doit s'assurer que les patchs critiques sont appliqués aux systèmes comme recommandé par les vendeurs de logiciels, après avoir été vérifiés par le Fournisseur pour compatibilité avec ses installations.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.12.6.1
ABR.SEC.A1015.0.59 - 1	Le Fournisseur doit mettre en place des mécanismes appropriés de prévention de perte des données afin d'éviter toute divulgation non autorisée d'informations Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.11 Exigences - Sécurité des Communications

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.60 - 1	Le Fournisseur doit respecter les normes et procédures de connexion et d'échange de données Airbus, sauf spécification écrite contraire de la part d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.13.2.1
ABR.SEC.A1015.0.61 - 1	Dans le cas de transfert de données Airbus par l'intermédiaire de réseaux de données qui ne sont pas sous le contrôle direct du Fournisseur (par exemple, lignes louées, Internet), le Fournisseur doit prendre toutes les mesures nécessaires pour assurer la confidentialité et l'intégrité des données en cours d'acheminement.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.13.2.2 ; ISO 27001-2013-A.13.1.1

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.62 - 2	Le Fournisseur doit s'assurer que le trafic de données vers et depuis Internet ou tout autre réseau non sécurisé (par exemple, des environnements de test, des réseaux partenaires) est limité à l'aide de mécanismes robustes de sécurité et contrôlé pour garantir l'absence de tout comportement anormal (par exemple, à l'aide de proxys et de passerelles). *Nota 1 : Les adresses Internet connues pour présenter un risque de mauvais usage ou être une source d'attaques sont bloquées. Les mêmes précautions doivent s'appliquer pour les e-mails potentiellement dangereux, comme le courrier indésirable, le hameçonnage (phishing) et les pièces jointes suspectes.* *Nota 2 : Le Fournisseur empêche également les utilisateurs de contourner ces mécanismes de contrôle (par exemple, des utilisateurs passant par d'autres proxys, utilisant des messageries web ou services de "cloud" personnels pour partager des données professionnelles ou télécharger des données non autorisées).*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.13.2.3
ABR.SEC.A1015.0.63 - 2	Le Fournisseur ne doit utiliser que les équipements qui ont été approuvés par Airbus pour se connecter aux réseaux, systèmes ou produits Airbus (à l'exception des "portails fournisseurs"). *Nota : Airbus peut surveiller et corriger par l'installation de patchs (y compris par des mises à jour contre les logiciels malveillants) les équipements sur son réseau. Les équipements propres du Fournisseur ne respectant pas cette exigence ne peuvent être connectés que sur des réseaux isolés d'Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.13.1.3

2.12 Exigences - Acquisition, Développement et Maintenance des Systèmes

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.64 - 2	Le Fournisseur doit s'assurer que les produits livrés à Airbus qui comprennent des composants des systèmes d'information, technologie opérationnelle ou Internet des objets (incluant, à titre non limitatif, les logiciels, les équipements de fabrication avec des composants informatiques intégrés, les systèmes de contrôle industriel et de gestion des bâtiments) sont développés à l'aide d'une méthodologie de développement structurée et approuvée garantissant que les exigences en matière de sécurité de l'information font partie du processus et sont par conséquent définies, documentées et respectées à l'aide de règles de codage et vérifiées dans la phase de test et de réception.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.14.2.1
ABR.SEC.A1015.0.65 - 2	Si les produits livrés à Airbus par le Fournisseur doivent être installés ou connectés à l'environnement des systèmes d'information, technologie opérationnelle ou Internet des objets connectés d'Airbus, le Fournisseur doit s'assurer qu'ils peuvent être intégrés dans les processus de sécurité réseau d'Airbus : protection contre les logiciels malveillants, gestion des vulnérabilités, application de patchs, contrôle des accès, suivi des incidents et journalisation. *Nota : Les produits livrés à Airbus par le Fournisseur qui comprennent des composants des systèmes d'information, technologie opérationnelle ou Internet des objets incluent, à titre non limitatif, les logiciels, les équipements de fabrication avec des composants informatiques intégrés, les systèmes de contrôle industriel et de gestion des bâtiments.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.66 - 2	Le Fournisseur doit s'assurer que sa maintenance à distance et son support sur les produits livrés à Airbus sont conformes aux normes de connexion à distance d'Airbus. *Nota : Les produits livrés à Airbus par le Fournisseur qui comprennent des composants des systèmes d'information, technologie opérationnelle ou Internet des objets connectés incluent, à titre non limitatif, les logiciels, les équipements de fabrication avec des composants informatiques intégrés, les systèmes de contrôle industriel et de gestion des bâtiments.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.9.1.2
ABR.SEC.A1015.0.99 - 1	Lorsque le Fournisseur doit connecter ses propres équipements de systèmes d'information, technologie opérationnelle ou Internet des objets connectés à l'un de ses propres produits au sein des systèmes de production d'Airbus ou intégré dans un produit Airbus (avion, hélicoptère, satellite, drone, etc...) aux fins de la configuration, du chargement de logiciels/de données, de test ou de dépannage dans les environnements de production, livraison ou maintenance d'Airbus, le Fournisseur doit s'assurer que ces équipements de systèmes d'information, technologie opérationnelle ou Internet des objets connectés et les logiciels qu'ils contiennent : – sont dédiés et limités à cette activité et que leur utilisation fait l'objet de procédures formelles, – ne sont pas connectés à un autre réseau que le réseau interne produit lors du fonctionnement au niveau du produit Airbus, – sont authentiques, intacts/exempts de défaut et de logiciel malveillant ; ceci inclut également tout support amovible connecté aux équipements.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.13 Exigences - Relations avec le Fournisseur

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.67 - 2	Si le Fournisseur a besoin d'autoriser l'un de ses sous-traitants à accéder aux informations Airbus, il doit en avertir Airbus et toutes les exigences spécifiées dans le présent document doivent être répercutées en cascade jusqu'au dernier sous-traitant par un accord particulier. *Nota 1 : Le Fournisseur est seul responsable de la mise en application des exigences de sécurité Airbus au sein de sa propre chaîne d'approvisionnement.* *Nota 2 : Outre les activités industrielles, cette exigence couvre également les fournisseurs d'externalisation/ de cloud des systèmes d'information, technologie opérationnelle ou Internet des objets connectés des Fournisseurs, la gestion des installation et services similaires avec accès aux Informations d'Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.68 - 2	Le Fournisseur doit communiquer l'accord concernant les exigences de sécurité entre le Fournisseur et un fournisseur et/ou sous-traitant de rang inférieur à Airbus sur demande. *Nota : Cet accord ne constituera en aucun cas une relation contractuelle directe entre Airbus et les fournisseurs et/ou sous-traitants du Fournisseur.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.69 - 2	Le Fournisseur doit réaliser des revues de sécurité et de risques afin de s'assurer du respect de la présente Directive par son sous-traitant. *Nota 1 : Le Fournisseur est également chargé de signaler tout constat de non-conformité au Département Sécurité d'Airbus.* *Nota 2 : Airbus se réserve le droit de réaliser une évaluation complémentaire des sous-traitants du Fournisseur par rapport à la présente Directive, cette évaluation pouvant être effectuée par le Département Sécurité d'Airbus ou par un auditeur indépendant agréé.* *Nota 3 : Le Fournisseur est autorisé à nommer un auditeur indépendant agréé pour cette tâche.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.2.1

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.70 - 2	En aucun cas, le Fournisseur ne doit octroyer l'accès aux systèmes ou données Airbus (y compris, mais non de façon limitative, l'acheminement ou le relais) à aucun de ses fournisseurs et/ou sous-traitants sans l'autorisation écrite préalable d'Airbus.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.14 Exigences - Gestion des Incidents Liés à la Sécurité de l'Information

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.71 - 1	Le Fournisseur doit assurer une surveillance continue des systèmes et réseaux, utiliser des moyens de détection et de prévention des intrusions et enregistrer les événements liés à la sécurité.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.72 - 1	Le Fournisseur doit mettre en place des contrôles appropriés pour identifier et contrer les cyber-attaques sophistiquées, comme les menaces persistantes avancées (APT), et les canaux de commande et de contrôle.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.73 - 2	Le Fournisseur doit mettre en place, pour les informations et les systèmes, un processus de gestion des incidents exhaustif et approuvé incluant l'identification, la réponse, la récupération, le reporting, la protection des preuves et l'examen consécutif à la mise en œuvre, en cas d'incidents liés à la sécurité de l'information. *Nota : Ces incidents incluent, à titre non limitatif : les équipements perdus ou volés, les anomalies de fonctionnement, les pannes d'alimentation, les surcharges, les erreurs commises par des utilisateurs ou par le personnel des systèmes d'information, technologie opérationnelle ou Internet des objets connectés, les violations d'accès, les logiciels malveillants et le piratage.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.16.1.1
ABR.SEC.A1015.0.74 - 2	Le Fournisseur doit identifier et résoudre les incidents et failles de sécurité, limiter leurs impacts commerciaux et réduire le risque d'occurrence d'incidents similaires.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.16.1.1

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.75 - 2	En cas d'incident lié à la sécurité et affectant potentiellement les systèmes ou informations Airbus, le Fournisseur doit réaliser une enquête et en communiquer les résultats au Département Sécurité d'Airbus sans délai, même si aucune demande n'a été formulée. *Nota : Ces incidents incluent, à titre non limitatif : le vol d'équipements stockant des informations Airbus, la fuite de données Airbus en provenance des systèmes du Fournisseur, la compromission des systèmes connectés à Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.2.1 ; ISO 27001-2013-A.16.1.2
ABR.SEC.A1015.0.76 - 2	Le Fournisseur doit prendre les mesures nécessaires pour remédier aux incidents de sécurité détectés ou signalés. *Nota : Si Airbus détecte dans ses systèmes un incident quelconque lié à la sécurité ayant pour origine le Fournisseur, Airbus en avertit immédiatement le Fournisseur et se réserve le droit de suspendre ou de restreindre temporairement la connexion au Fournisseur.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.16.1.5

2.15 Exigences - Aspects Liés à la Sécurité de l'Information Concernant la Gestion de la Continuité Opérationnelle

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.77 - 2	Le Fournisseur doit avoir préparé un Programme de Continuité Opérationnelle afin d'assurer le maintien/rétablissement des services liés aux systèmes d'information, technologie opérationnelle ou Internet des objets connectés en cas de panne majeure ou en cas de force majeure, de toute nature (y compris, mais non de façon limitative, dommages matériels, coupures de courant, incendie, catastrophe naturelle). *Nota : Ce programme comporte les éléments suivants : Cadre de gestion, Plans de continuité opérationnelle, Suivi, revue et essais, Reprise des activités après sinistre.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.17.1.1
ABR.SEC.A1015.0.78 - 1	Cadre de gestion - Le Fournisseur doit avoir mis en place les processus et mécanismes appropriés, avoir défini les rôles et responsabilités pour assurer la continuité des processus opérationnels et éviter des perturbations majeures. *Nota : Ceci doit englober l'identification et l'évaluation des Risques, les stratégies d'atténuation de ces risques, le maintien de la disponibilité des services, des processus et des produits de l'activité à travers la sensibilisation, les revues et les essais.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.17.1.1
ABR.SEC.A1015.0.79 - 1	Plans de continuité opérationnelle - Le Fournisseur doit documenter et former ses employés aux plans de continuité opérationnelle afin d'assurer une poursuite efficace des activités en cas d'incident majeur.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.17.1.2
ABR.SEC.A1015.0.80 - 1	Suivi, revue et test - Le Fournisseur doit être en mesure de prouver l'existence d'une revue, d'un suivi et de tests périodiques des plans par le biais d'exercices.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.17.1.3
ABR.SEC.A1015.0.81 - 2	Reprise des activités après sinistre - Le Fournisseur doit établir un plan de Reprise des Activités après Sinistre pour son activité liée à Airbus et les systèmes et processus internes qui en dépendent. *Nota : Ce plan couvre la planification et la description détaillée des mesures à prendre pendant et après un incident, de telle sorte que les opérations puissent reprendre dans des conditions redevenues normales.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.17.1.2

2.16 Exigences - Conformité

Airbus et le Fournisseur s'engagent tous deux à respecter toutes les exigences réglementaires pertinentes (en particulier lorsque le dispositif d'accès est international et couvre différentes juridictions). Ces exigences varient en fonction de la nature du Fournisseur et sont susceptibles de révision au cas par cas.

On accordera une attention particulière aux conflits de lois liés notamment à la protection/au caractère personnel/confidentialité des données, au contrôle, à la rétention de données et à la cryptographie.

Le Fournisseur prend acte du fait que le Département Sécurité d'Airbus ou un auditeur indépendant désigné par Airbus peut procéder à un audit de la sécurité des systèmes, processus et procédures du Fournisseur, dès lors que des informations ou systèmes Airbus sont mis en place ou accessibles chez ce Fournisseur.

Airbus se réserve le droit, sur préavis raisonnable, de procéder à des audits de conformité et/ou de mise en œuvre, à sa discrétion.

Airbus se réserve le droit de suspendre ou de restreindre la connexion du Fournisseur ou son accès aux informations dans les cas où l'accès pour les besoins de l'audit a été refusé ; les actions correctives n'ont pas été mises en œuvre ; en cas de manque de coopération en cas d'incident majeur lié à la sécurité.

En cas de modification significative de la situation du Fournisseur (y compris, mais non de façon limitative, fusion, acquisition ou autre réorganisation de l'entreprise) ou de ses activités commerciales, Airbus se réserve le droit de réévaluer la conformité du Fournisseur avec les exigences de sécurité Airbus selon besoin afin de protéger les informations et les infrastructures associées à Airbus.

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.82 - 1	Le Fournisseur doit assurer la révision et l'audit réguliers : – de la robustesse technique de ses systèmes ; – de la conformité à la politique ; – des procédures de sauvegarde des systèmes et des informations.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.18.2.1
ABR.SEC.A1015.0.83 - 1	Le Fournisseur doit respecter tous les règlements et lois en vigueur sur le droit d'auteur/la propriété intellectuelle et obtenir toutes les licences de logiciels nécessaires.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.18.1.2

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.84 - 2	Le Fournisseur doit autoriser Airbus (ou un auditeur indépendant agréé) à accéder aux bâtiments, documents, systèmes, etc..., pour les besoins de l'inspection et de la validation des dispositifs de sécurité, conformément à la présente Directive, et en vue de la réduction des risques généraux liés à la sécurité de l'information. *Nota : Cette autorisation d'accès peut également être répercutée dans la chaîne d'approvisionnement du Fournisseur lorsqu'il est présumé que l'échange de données et la connexion des systèmes s'effectuent avec les systèmes Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.2.1
ABR.SEC.A1015.0.85 - 1	Le Fournisseur doit prendre toutes dispositions utiles pour fournir à Airbus les informations appropriées nécessaires à la réalisation d'une évaluation de sécurité par Airbus ou par un auditeur indépendant agréé.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.15.2.1
ABR.SEC.A1015.0.86 - 1	Le Fournisseur doit prendre toutes les mesures correctives appropriées concernant toute anomalie identifiée par l'audit.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.88 - 2	Le Fournisseur doit pouvoir apporter à Airbus la preuve que son organisation répond aux lois et aux réglementations applicables en matière d'exportation, et doit assurer la traçabilité de ces preuves afin de pouvoir satisfaire à tout contrôle. *Nota : Airbus pourra contrôler à tout moment la fiabilité de l'organisation du Fournisseur au regard de ces exigences (physiques et logiques). Ceci inclut, mais non de façon limitative, la vérification de l'identité et de la(des) nationalité(s) des utilisateurs, l'autorisation et le contrôle d'accès aux informations (avec une procédure formelle d'agrément des utilisateurs), le contrôle du flux de l'information et les pistes d'audit.*	Fournisseur - Fournisseur d'Airbus pour tous types de biens, données techniques ou services soumis aux lois et règlementa-tions sur le contrôle des exportations.	Airbus internal

Référence	Description	Applicabilité	Origine
ABR.SEC.A1015.0.90 - 2	Lorsque, dans le cadre de son contrat, le Fournisseur doit avoir accès à des informations soumises à une classification défense, gouvernementale, OTAN ou OCCAR, le Fournisseur doit mettre en place tous les moyens techniques et organisationnels lui permettant de se conformer à la loi sur les secrets nationaux du pays où le contrat est exécuté, en conformité avec les niveaux de classification fournis par Airbus dans l'instruction spécifique de sécurité des programmes ou la lettre sur les aspects de sécurité.	Fournisseur - Fournisseur d'Airbus pour tout type de biens, de données techniques ou de services soumis à une classification défense, gouvernemen-tale, OTAN ou OCCAR	Airbus internal
ABR.SEC.A1015.0.91 - 1	Le Fournisseur doit transmettre à Airbus tous les renseignements nécessaires et l'assurer de sa coopération en cas d'assignation, d'enquête ou autre visant à obtenir des informations Airbus, et doit transmettre à Airbus tous les renseignements et l'assistance nécessaires pour obtenir la certification ou autre de ses informations, y compris les informations en possession du Fournisseur.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal
ABR.SEC.A1015.0.92 - 2	Le Fournisseur doit avertir sans délai Airbus de la réception de toute demande nécessitant la fourniture d'informations Airbus à un tiers, y compris aux administrations ou autorités. *Nota : Le Fournisseur fait appel à tous les moyens légaux pour contester une telle demande, sauf si elle a été approuvée par Airbus.*	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

2.17 Exigences - Fin du Contrat/Désengagement

Référence	Description	Applicabilité	Origine
ABR.SEC.A1015.0.93 - 1	Au moment de la signature du contrat, ou avant cette date, le Fournisseur doit transmettre à Airbus un plan de fin de contrat qui stipule la manière dont les informations Airbus, y compris les sauvegardes et archives, seront rendues à Airbus à la fin du contrat et la manière dont les informations Airbus seront définitivement effacées des équipements et installations du Fournisseur.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.94 - 1	Le Fournisseur doit assurer la protection des systèmes et informations Airbus, y compris le maintien du service, à l'expiration du Contrat/des dispositions contractuelles et conformément aux clauses du Contrat/ des dispositions contractuelles.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	Airbus internal

Référence	***Description***	***Applicabilité***	***Origine***
ABR.SEC.A1015.0.95 - 1	Le Fournisseur est tenu d'aviser immédiatement Airbus lorsque l'accès à certains ou à tous les systèmes ou données Airbus n'est plus nécessaire pour s'acquitter de ses obligations au titre du Contrat/des dispositions contractuelles.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.96 - 1	A l'expiration de la période convenue d'utilisation des informations ou si les informations ne sont plus nécessaires, le Fournisseur doit éliminer les informations selon la méthode convenue avec Airbus et s'assurer que celles-ci ne peuvent être récupérées.	Fournisseur - Fournisseur d'Airbus pour tout type de biens ou services	ISO 27001-2013-A.8.1.4

3 Documents de Référence

Les documents listés dans ce qui suit ont servi à la rédaction de la présente Directive. Ils ne peuvent cependant pas être considérés comme partie intégrante d'un Contrat/de dispositions contractuelles entre Airbus et le Fournisseur reposant sur cette Directive, sauf mention contraire et explicite dans la clause correspondante. Airbus transmettra au Fournisseur les documents de référence sur demande.

Nota : Le Fournisseur doit se procurer directement les documents ISO ou ISF, Airbus ne pouvant fournir ces documents pour des raisons de droit d'auteur.

Référence du Document	***Titre***
A1044	Security Requirements for Classification & Protection of Information
GTC	General Terms and Conditions for Access to and Use of Airbus Supplier Portals
ICT/IST Charter	Airbus Information Managements - Use of IST Facilities
ISO/CEI 27001	Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences
ISO/CEI 27002	Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information
ISO/CEI 27003	Technologies de l'information - Techniques de sécurité - Sécurité de l'information
ISO/CEI 27036	Technologies de l'information - Techniques de sécurité - Lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information
CEI 62443 Part 2-1 2010	Réseaux industriels de communication - Sécurité dans les réseaux et les systèmes - Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles
SoGP Avril 2016	The ISF Standard of Good Practice for Information Security

4 Glossaire

Toujours se référer au LEXINET

Airbus	Désigne Airbus S.A.S. et ses filiales, joint-ventures, sociétés affiliées et associées
Informations Airbus	Dans le cadre de la présente Directive, désigne les droits de propriété intellectuelle d'Airbus, ainsi que les méthodes, le savoir-faire, la technologie et les procédés exclusifs et/ou protégés, les faits et chiffres internes, et tout matériel ou document associé. Ceci inclut tous les moyens et méthodes de stockage et de transmission possibles, sous quelque forme que ce soit et quel qu'en soit le support (y compris, mais non de façon limitative, les documents papier, sorties imprimées, microfiches, données électroniques sous toute forme, photographies et multimédias)

Sécurité Airbus	Dans le cadre de la présente Directive, désigne l'organisation et les personnes chez Airbus responsables de la protection du personnel, des activités, du patrimoine scientifique et technologique, des actifs et de la réputation d'Airbus contre toutes les actions hostiles, de manière à prévenir, détecter et répondre à ces actions
Continuité Opérationnelle	Dans le cadre de la présente Directive, désigne la capacité stratégique et tactique de l'organisation du Fournisseur à prévoir et intervenir en cas d'incidents et de perturbations des activités afin que les opérations commerciales se poursuivent à un niveau acceptable pour garantir l'exécution du contrat
Cyber	Dans le cadre de la présente Directive, préfixe se rapportant à Internet et aux réseaux de télécommunications, monde dynamique technologiquement interconnecté en permanence qui comprend des personnes, des organisations, des données et des technologies. Ce monde évolue constamment de manière imprévisible, facilite la coopération, mais minimise les risques pour les activités criminelles, concentre les cibles et permet aux auteurs de ces crimes de se dissimuler
Données	Dans le cadre de la présente Directive, désigne toutes les informations électroniques, sous quelque forme que ce soit et quel qu'en soit le support
Sécurité de l'information	Correspond à la protection des éléments suivants : – Disponibilité - Afin d'éviter toute perte d'informations et de services, résultant, par exemple, de l'utilisation d'un code malveillant, de catastrophes naturelles, de fonctionnements défectueux/pannes systèmes. – Intégrité - Afin d'éviter tout traitement, saisie, modification, suppression non autorisés. – Confidentialité - Afin d'éviter toute divulgation non autorisée. – Imputabilité - Afin de garantir l'identité des utilisateurs, la responsabilité individuelle et les pistes d'audit en matière d'accès et de transactions, ceci afin de prévenir et de détecter toute intrusion frauduleuse
SI (système d'information)	Dans le cadre de la présente Directive, désigne, en lien avec les technologies de l'information et les télécommunications, les équipements, services, logiciels et processus associés utilisés pour le stockage, le traitement et la transmission de données. Ce terme désigne notamment, les PC, stations de travail, ordinateurs portables, supports de stockage amovibles, téléphones, smartphones, réseaux, systèmes, programmes informatiques, serveurs, bases de données et portails web
ISF	Information Security Forum
ISMS	Information Security Management System (système de gestion de la sécurité de l'information)
OTAN	Organisation du traité de l'Atlantique Nord
OCCAR	Organisation Conjointe de Coopération en matière d'Armement OTAN
Technologie opérationnelle (OT)	Dans le cadre de la présente Directive, désigne les équipements, services, logiciels, progiciels et processus associés de technologie de gestion des données ou de communication, utilisés pour le stockage, le traitement et la transmission de données intégrés dans des équipements de fabrication (OT). Cela inclut notamment les interfaces homme-machine, les interfaces frontales, les supports amovibles, les réseaux, les automates utilisés dans les systèmes de contrôle de fabrication et de gestion des bâtiments

Risque	Dans le cadre de la présente Directive, désigne un événement ou un état qui, le cas échéant, est susceptible d'avoir des répercussions négatives sur les objectifs et sur l'exécution du contrat du Fournisseur en termes de conception, de production et/ou livraison future des produits/services à Airbus
Gestion des Risques	Désigne un processus de gestion prospective qui anticipe les risques éventuels pour les objectifs commerciaux du Fournisseur et prévoit leur réduction, de telle sorte que les systèmes d'information ne soient pas eux-mêmes exposés (ou n'affectent pas, à leur tour, les processus opérationnels supportés) aux conséquences qui auront été raisonnablement prévues et évitées
Fournisseur	Dans le cadre de la présente Directive, désigne les entités fournissant des biens et/ou des services au profit d'Airbus, mais ne faisant pas partie d'Airbus (y compris, mais non de façon limitative, les fournisseurs, les sous-traitants, les partenaires industriels et les centres de recherche)
Internet des objets (IoT)	Dans le cadre de la présente Directive, désigne le réseau de dispositifs physiques, véhicules et autres éléments incluant des moyens électroniques, logiciels, capteurs, actionneurs ainsi qu'une connexion réseau permettant à ces objets de collecter et d'échanger des données. Chaque objet est identifiable de manière unique via le son système informatique intégré mais est capable d'interagir au sein d'une infrastructure Internet existante

Collaborateurs

Nom	***Fonction***
ALTSTÄDT Kai	Prod. Indust & Operational Security MGR - EIDS
BALLARD Florence	Security Business Partners - ZSB
BOUDET Florent	Security Assurance - ZSG
DENIS Pierrette	Security Operations - ZSO
GAUVRY Philippe	Q Procurement Requirements Proj Mgr - QPR
JORDAN Marie	Prod. Secur capabilities Compliance MGR - EIDC1
MEIER-HEDDE Felix	Prod. Indust & Operational Security MGR - EIDS
REY Nathalie	Prod. Indust & Operational Security MGR - EIDS
THORNARY Mathieu	IM Security Analyst - ZIST
TREDEZ Juliette	Governance - ZSG
UTH Fridtjof	Security Assurance - ZSG

Acceptable Translation for Deployment in the Local Language

Function	***Name***	***Date***
Validation of English Translation	**TREDEZ Juliette**	**22/02/18**

Tableau d'Evolution

Indice	***Date***	***Synthèse et justification des modifications***
A	Déc 2017	Edition initiale. Refonte du document. Fusion du document A1015 Airbus et de l'ancien E260 Airbus Group, comprenant les exigences Airbus Helicopters et Airbus Defence&Space, et les aspects produit/OT.
	Fév 2018	**La traduction en français est disponible.**

Informationssicherheits-Forderungen für Lieferanten

ZWECK/GELTUNGSBEREICH:

Diese Direktive legt die Airbus-Sicherheits- und Risikomanagement-Anforderungen für Lieferanten fest. Zweck dieser Directive (Richtlinie) A1015.0 (im Folgenden "Direktive" genannt) ist die Aufrechterhaltung der Sicherheit von Airbus-Geschäftsinformationen, Informationsverarbeitungssystemen, Produkte und Einrichtungen der Airbus-Organisation, auf die Lieferanten und deren eigene Lieferanten zugreifen bzw. die sie betreiben oder verarbeiten werden, die sich sowohl an Airbus-Standorten als auch außerhalb hiervon befinden.

Airbus Procurement muss die in dieser Direktive festgelegten Airbus-Anforderungen zur Informationssicherheit ohne Ausnahme auf alle Lieferantenverträge/vertraglichen Vereinbarungen mit Lieferanten anwenden, die mit beliebigen Airbus-Entities, -Standorten und Werken einschließlich Tochtergesellschaften und Joint-Ventures geschlossen werden, an denen Airbus mehrheitlich beteiligt ist. Diese Direktive kann mittels zusätzlicher Sicherheitsspezifikationen in Bezug auf die beauftragten Arbeiten oder beschafften Produkte ergänzt werden, wenn dies durch die Sensitivität von Informationen/Konnektivität bzw. durch gültige interne und externe Vorschriften gefordert ist.

Herausgabeverantwortlicher des Dokuments:

Name: KNUEPPEL Dietrich

Funktion: Directive Owner

Freigabeverantwortlicher für die Anwendung:

Name: ANDREI Pascal

Funktion: SEC FoR Owner

INHALTSVERZEICHNIS

1 Einführung

Es besteht eine zunehmende unternehmerische Notwendigkeit, Airbus-Lieferanten direkten oder integrierten Zugriff auf Airbus-Informationen und Informationssysteme und somit auf dessen Daten zu gewähren, dem Unternehmen ist jedoch bewusst, dass Airbus hierdurch einer Vielzahl von Risiken ausgesetzt ist. Sinn und Zweck dieser Direktive ist es festzulegen, wie die Auftragnehmer arbeiten müssen, um eine vertrauensvolle Zusammenarbeit aufzubauen.

Airbus ist bewusst, dass sich aus der Bereitstellung des Zugriffs auf Informationen und Informationssysteme für Lieferanten Risiken ergeben durch:

- den Verlust der Kontrolle darüber, wo Auftragnehmer auf Airbus-Informationen und Informationssysteme zugreifen bzw. diese betreiben.
- den Verlust der Kontrolle und Verantwortlichkeit dort, wo Airbusinformationen und Informationssysteme extern angesiedelt sind.
- den Verlust der Transparenz der Aktivitäten des Lieferanten bezogen auf Airbus-Sicherheitszwänge.

Man ist sich auch darüber bewusst, dass ein unzureichender Schutz der eigenen Daten und Systeme des Lieferanten sowohl die Qualität als auch die termingerechte Auslieferung von Waren oder Dienstleistungen an Airbus gefährden kann. Es besteht somit auch aus industrieller Sicht die Anforderung nach einer angemessenen Sicherheit der Informationssysteme, Betriebstechnik (OT) bzw. des Internets der Dinge (IoT) und Notfallvorsorge des Lieferanten.

Die in dieser Direktive aufgeführten Anforderungen müssen daher in allen der folgenden Anwendungsfälle umgesetzt werden:

- Der Lieferant greift (per Fernzugriff oder vor Ort) mittels Informationstechnik auf die Informationssysteme, Betriebstechnik (OT) oder Produkte von Airbus zu,
- Der Lieferant verfügt in seinen Systemen über Airbus-Informationen,
- Der Lieferant nutzt seine eigenen IT-, OT- bzw. IoT-Systeme für die Herstellung, Lieferung, Installation, Instandhaltung von Produkten bzw. für die Erbringung von Dienstleistungen an Airbus.

Des Weiteren wird die Datensicherheit in kooperativen Projekten sowie beim internen Informations- und Datenaustausch in Europa und den USA zunehmend durch Regierungsstellen überwacht.

Cyber-Spionage stellt ebenfalls eine erhebliche und wachsende Bedrohung für Unternehmen dar, die mit speziellen Schlüsselindustrien wie der Luft- und Raumfahrt- und Verteidigungstechnologie arbeiten. Weitentwickelte Cyber-Abwehrmechanismen bei Airbus bieten ein bestimmtes Maß an Schutz, aber Bedrohungen können auch aus der Lieferkette hervorgehen. Lieferanten haben Zugriff auf Airbus-Informationen und -Systeme, aber ihnen fehlt möglicherweise die entsprechende Sicherheitsinfrastruktur, um die Informationsgüter angemessen zu schützen, wodurch sie dann einen passiven Verstoß gegen die getroffene(n) Geheimhaltungsvereinbarung(en) riskieren.

Airbus setzt sich dafür ein, die entsprechenden Bedürfnisse durch ein angemessenes Sicherheitsniveau in seiner Lieferkette widerzuspiegeln.

2 Anforderungen

2.1 Anforderungen - Vereinbarung über kooperatives Arbeiten (Collaborative Working)

Airbus strebt eine Kooperation mit Lieferanten in Übereinstimmung mit beiderseitig einzuhaltenden Vorschriften/Vereinbarungen an.

Dieses Dokument gilt ergänzend zu den allgemeinen Zugangs- und Nutzungsbedingungen für Airbus-Supplier-Portale ("General Terms and Conditions (GTC) for Access to and Use of Airbus Supplier Portals").

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.1 - 2	Der Lieferant muss sich verpflichten, professionell zu arbeiten und die in diesem Dokument enthaltenen Sicherheitsanforderungen guten Glaubens zu erfüllen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.1.2; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.2 - 1	Der Lieferant ist für seine täglichen Betriebsabläufe mit Airbus-Systemen und -Informationen in Übereinstimmung mit dieser Direktive verantwortlich.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.1.2; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.3 - 1	Vor bzw. ab der Umsetzung des Vertrages/ der vertraglichen Regelungen mit Airbus muss der Lieferant einen Grundschutz in Übereinstimmung mit dieser Direktive eingerichtet haben.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.1.2; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.4 - 2	Der Lieferant ist für die Einführung geeigneter allgemeiner Sicherheitsrisikomanagement-Prozesse verantwortlich und gewährleistet, dass seine Unterauftragnehmer/Lieferanten innerhalb ihrer Organisationen ebenfalls solche ICT-Risikomanagement-Prozesse anwenden. *Anmerkung 1: Der Lieferant bewertet in regelmäßigen Abständen die Sicherheitsrisiken für Airbus neu, da die Möglichkeit besteht, dass neue Schwachstellen aufgedeckt werden, die Bedrohungslandschaft sich weiterentwickelt, Organisationsstrukturen sich verändern und die Technologie voranschreitet.* *Anmerkung 2: Der Lieferant pflegt ein Risiko-Register und einen Maßnahmenplan (hinnehmen, mindern, vermeiden oder übertragen) und Benachrichtigen von Airbus zu Sicherheitsrisiken in Bezug auf die gelieferten Dienstleistungen bzw. Waren.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.5 - 2	Der Lieferant darf nur mit entsprechender Genehmigung von Airbus auf jegliche Funktionen von Airbus-Systemen oder auf Airbus-Daten zugreifen, sie nutzen, verändern und/oder löschen. *Anmerkung: Der Lieferant versucht nicht, auf Systeme oder Informationen zuzugreifen, die nicht von Airbus für die Vertragsdurchführung freigegeben worden sind.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.6 - 1	Der Lieferant darf nicht versuchen, Sicherheitsmechanismen des Netzwerkes und/oder der Systeme von Airbus zu umgehen, ändern oder deaktivieren.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.1.2
ABR.SEC.A1015.0.7 - 2	Der Lieferant ist dafür verantwortlich sicherzustellen, dass nicht gegen maßgebliche Airbus-Sicherheitsgrundsätze (z.B. Regeln betreffend die zulässige Nutzung von Airbus-Systemen/ICT Charter, Betriebsordnung für Besucher, Mitarbeiter am Standort, usw.) verstoßen wird, es sei denn es liegt eine schriftliche Einwilligung seitens der Airbus Security-Organisation vor. *Anmerkung: Das Arbeiten an bestimmten Airbus-Standorten oder -Projekten kann eine behördliche Zulassung des Lieferanten (Sicherheitsbescheid) erfordern.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.11.1.5
ABR.SEC.A1015.0.97 - 1	Der Lieferant muss sämtliche entsprechenden Airbus-Informationen, auf die er zugreift, mit denen er arbeitet oder die er verarbeitet vor Verlust, Vernichtung, Verfälschung, Datenkorruption, unberechtigtem Zugriff und unbefugte Offenlegung schützen. *Anmerkung: Dieser Schutz bleibt auch nach Vertragsende bestehen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

2.2 Anforderungen - Erste Bewertung

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.8 - 2	Vor Einrichtung eines Datenaustauschs oder der Anbindung an Systeme oder Netzwerke muss der Lieferant der Airbus Security alle erforderlichen Informationen und Dokumentationen zur Verfügung stellen, um eine Beurteilung des Sicherheitsniveaus des Lieferanten im Hinblick auf diese Directive zu ermöglichen. *Anmerkung 1: Dies soll ein Exemplar seiner aktuellen Informationssicherheitsgrundsätze umfassen, und zwar einschließlich seiner Regularien hinsichtlich der physischen Sicherheit beim Zugang zu Räumlichkeiten oder Einrichtungen, in denen eine Verbindung mit Airbus-Systemen hergestellt werden kann bzw. Airbus-Informationen verarbeitet werden können.* *Anmerkung 2: Airbus stellt die vertrauliche Behandlung aller vom Lieferanten bereitgestellten Informationen sicher.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.1.1

2.3 Anforderungen - Sicherheitsleitlinien

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.10 - 1	Der Lieferant muss formell das Engagement des Managements sowie effizientes Benutzer-Bewusstsein sicherstellen, indem er umfassende und genehmigte Informationssicherheitsregularien und Benutzerrichtlinien entwickelt und an alle Personen verteilt, die Zugang zu den Informationen des Lieferanten sowie dessen Systeme haben.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.5.1.1
ABR.SEC.A1015.0.11 - 1	Auf der Grundlage der Informationssicher-heitsregularien muss der Lieferant ein umfassendes Werk aus betrieblichen Standards und Verfahrensanweisungen für die Zielgruppe der privilegierten Nutzer (z.B. Administratoren und Programmierer) erstellen, um eine durchgängige Umsetzung von Informationssicherheitsmaßnahmen zu gewährleisten.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.5.1.1

2.4 Anforderungen - Organisation der Sicherheit

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.12 - 2	Ernennung eines Security Managers - Der Lieferant muss einen Mitarbeiter mit der Gesamtverantwortung für Sicherheits- und Risikothemen benennen und diese Funktion mit den entsprechenden Befugnissen und Mitteln ausstatten, um die Aktivitäten in der gesamten Organisation zu koordinieren.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.6.1.1
ABR.SEC.A1015.0.13 - 1	Der Security Manager des Lieferanten muss alle geltenden und die Sicherheitsmaßnahmen, Prozesse und Systeme des Lieferanten betreffenden gesetzlichen und vertraglichen Vorgaben - u.a. die in dieser Direktive und in den Exportbestimmungen festgelegten - beachten.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.18.1.1
ABR.SEC.A1015.0.14 - 2	Der Lieferant muss gegenüber der Airbus Security einen Ansprechpartner in seiner Organisation sowie eine Ersatzperson benennen, der für die regelmäßige und vorfallsbezogene Berichterstattung verantwortlich ist.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.15 - 2	Der Lieferant muss Aufgaben und Verantwortlichkeiten in den Bereichen Sicherheit und Informationstechnik, Betriebstechnik (OT) bzw. IoT und Notfallvorsorge trennen, um das Risiko eines versehentlichen oder vorsätzlichen Missbrauchs von Systemen oder Anwendungen Internet der Dinge zu mindern.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.6.1.2

2.5 Anforderungen - Personelle Sicherheit

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.16 - 2	Der Lieferant ist allein verantwortlich für die Umsetzung der Airbus-Sicherheitsanforderungen innerhalb seiner Organisation und stellt daher sicher, dass die Benutzer qualifiziert und sachgemäß geschult sind.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.17 - 2	Der Lieferant muss systematische Prozesse zur Sicherheitsüberprüfung seiner Mitarbeiter etabliert haben, um deren Identität und Hintergründe zu überprüfen. *Anmerkung 1: Hierzu gehört auch die Überprüfung des höchsten Abschlusszeugnisses, der Wohnsitzadresse der letzten Jahre, der Referenzen früherer Arbeitgeber, der Gültigkeit vorgelegter Ausweisdokumente sowie die Abwesenheit schwerer strafbarer Handlungen.* *Anmerkung 2: In Ländern, in denen ein solcher Prozess durch Gesetze und Vorschriften Einschränkungen unterliegt, führt der Lieferant die Sicherheitsüberprüfung in dem durch die Gesetze und Vorschriften zulässigen vollen Umfang durch.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.18 - 1	Auf Anfrage muss der Lieferant Informationen aus der Sicherheitsüberprüfung seiner Mitarbeiter bereitstellen. *Anmerkung: Im Falle von Arbeiten, die staatlichen Verordnungen unterliegen oder von anderen vertraulichen Projekten behält sich Airbus ggf. das Recht vor, im Rahmen der gesetzlich zulässigen Möglichkeiten Sicher-heitsüberprüfungsinformationen anzufordern.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.19 - 1	Der Lieferant muss sicherstellen, dass sämtliche Mitarbeiter und Lieferanten/ Unterauftragnehmer, die Zugang zu Airbus-Informationen und -Daten haben, auf den vertraulichen Charakter dieser Informationen hingewiesen werden und über die in dieser Direktive enthaltenen Verpflichtungen in Kenntnis gesetzt werden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.2.2
ABR.SEC.A1015.0.20 - 2	Der Lieferant muss sicherstellen, dass die Verträge mit seinen Mitarbeitern und Lieferanten/Unterauftragnehmern die in dieser Directive enthaltenen Verpflichtungen zur Vertraulichkeit erfüllen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.1.2

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.21 - 2	Der Lieferant muss Beauftragte für das Management und die Sicherheit von ICT-Systemen benennen und Airbus bei Änderungen dieser Mitarbeiter unverzüglich in Kenntnis setzen. *Anmerkung: Der Lieferant verpflichtet sich, dass Mitarbeiter, die andere Mitarbeiter ersetzen, mit Sachkunde und Befugnissen in vergleichbarem Umfang ausgestattet sind.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.22 - 1	Für den Fall, dass in Bezug auf einen Mitarbeiter des Lieferanten ein Sicherheitsproblem identifiziert wird, ist Airbus berechtigt, den Lieferanten davon in Kenntnis zu setzen, dass Airbus die Einteilung dieses Mitarbeiters des Lieferanten für Arbeiten in Zusammenhang mit Airbus missbilligt. Der Lieferant muss dann alle erforderlichen Schritte unternehmen, um sicherzustellen, dass dieser Mitarbeiter keinen Zugang zu geschützten oder vertraulichen Werten erhält, die dem Lieferanten in Zusammenhang mit seiner Arbeit für Airbus bereitgestellt werden. *Anmerkung: Zu den o.g. Werten zählen u.a. Informationen, Dokumente und Daten, jegliches Informationssystem (Hardware und Software) oder physische Produkte.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.7.2.3

2.6 Anforderungen - Management von Werten (Assets)

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.23 - 2	Der Lieferant muss Informationen, die zwischen ihm und Airbus transferiert werden, als Informationen mit dem Schutzvermerk "Airbus internal" erachten (siehe A1044 - Protection and Classification of Information Directive) und entsprechend sichern. *Anmerkung: Der Zugriff auf Informationen höherer Vertraulichkeitsstufen wird gesondert vereinbart.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.13.2.2; ISO 27001-2013-A.8.2.1; ISO 27001-2013-A.8.2.2
ABR.SEC.A1015.0.24 - 1	Der Lieferant muss hinsichtlich Airbus-Informationsklassifizierungen Verfahren für die Handhabung der Informationen einführen und bei den Nutzern das Bewusstsein hierfür fördern (siehe A1044 - Protection and Classification of Information Directive).	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.2.3

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.25 - 2	Der Lieferant muss eine aktuelle Liste der autorisierten IT, OT- bzw. IoT-Geräte führen, die verwendet werden, um auf Airbus-Informationen zuzugreifen, um diese zu transferieren, zu verarbeiten und/oder zu speichern.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.26 - 1	Auf Anfrage muss der Lieferant Airbus eine Liste aller Systeme und Einrichtungen bereitstellen, in denen Airbus-Informationen gespeichert bzw. verarbeitet werden (d.h. physischer Standort, Position im Netzwerk und Geschäftszweck der Speicherung/ Verarbeitung).	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.27 - 1	Für den Fall, dass der Lieferant nach ISO 27001 zertifiziert ist, muss er Airbus-Informationen und Anbindungen an Airbus-Systeme zum Verzeichnis der ISMS-Werte hinzuzufügen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.28 - 2	Der Lieferant darf Airbus-Informationen nicht auf mobilen Geräten speichern (Smartphones, Laptops, USB-Laufwerke, etc.), es sei denn sie sind mit Hilfe von dem Stand der Technik entsprechenden Produkten/Standards verschlüsselt.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.1.3
ABR.SEC.A1015.0.29 - 1	Gebrauchte oder defekte Speichermedien, auf denen Airbus-Informationen enthalten sind, müssen vor ihrer Ausmusterung bzw. Wiederverwendung erfolgreich gelöscht bzw. zerstört worden sein.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.3.2

2.7 Anforderungen - Zugriffskontrolle

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.30 - 2	Der Lieferant darf nur die von Airbus bereitgestellten oder geforderten Zugriffsmethoden und -kontrollen anwenden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.1.1
ABR.SEC.A1015.0.31 - 1	Der Lieferant muss die Verbindungen mit Airbus-Netzwerken und -Systemen ordnungsgemäß identifizieren und aufzeichnen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.32 - 1	Der Lieferant muss ein logisches Netzwerkdiagramm führen, in dem externe Verbindungen berücksichtigt und insbesondere die Verbindung zu Airbus aufgeführt ist.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.33 - 2	Der Lieferant muss eine aktuelle Liste der Benutzerautorisierungen für Systeme seines Betriebs pflegen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.34 - 2	Der Lieferant muss sicherstellen, dass der Benutzerantrags- und Autorisierungsprozess für Zugriffsrechte auf seine eigenen sowie auf Airbus-Systeme innerhalb seiner Organisation nachvollziehbar ist und nach dem Prinzip "Kenntnis nur wenn nötig" erfolgt.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.35 - 1	Der Lieferant muss Zugriffsrechte von Benutzern des Lieferanten unverzüglich entziehen, wenn diese aus beruflichen oder vertraglichen Gründen keinen Zugriff mehr auf Airbus-Systeme und/oder -Informationen benötigen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.36 - 1	Der Lieferant muss Airbus umgehend über solche Widerrufe in Kenntnis setzen, wenn hierzu eine administrative Maßnahme durch Airbus erforderlich ist.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.37 - 3	Der Lieferant muss mindestens in jährlichen Abständen attestieren, dass seine Benutzer von Airbus-IT-, OT- bzw. IoT-Systemen gemäß vertraglicher Festlegung berechtigt und befugt sind. *Anmerkung: Der Lieferant legt die Liste der Systembenutzer gegenüber dem für den Vertrag bzw. das Arbeitspaket zuständigen Vertragspartner (Business Owner) bei Airbus offen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.5

Referenz	Beschreibung	Voraussetzung für die Anwendbarkeit	Ursprung
ABR.SEC.A1015.0.38 - 3	Der Lieferant muss sicherstellen, dass die Zugriffe auf Systeme und Netzwerke protokolliert und die Protokolle mindestens 12 Monate lang aufbewahrt werden. *Anmerkung 1: Der Lieferant ergreift geeignete Maßnahmen, um sicherzustellen, dass Transaktionen nicht abgestritten werden können.* *Anmerkung 2: In Ländern, in denen die Aufbewahrung von Protokolldaten durch Gesetze und Vorschriften auf weniger als 12 Monate beschränkt ist, schöpfen die Lieferanten die in den Gesetzen und Vorschriften festgelegte Höchstdauer der Aufbewahrung voll aus.* *Anmerkung 3: Das Protokoll umfasst auch die Einrichtung/Änderung/Entziehung von Zugriffsrechten und Berechtigungsnachweisen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.4.1
ABR.SEC.A1015.0.39 - 1	Der Lieferant muss sicherstellen, dass Benutzer mit erhöhten Zugriffsrechten (z.B. Administratoren) zusätzlich zur Protokollierung ihres System- und Netzwerkzugriffs und der Nutzung ihrer Berechtigung auch im Hinblick auf regelwidrige Aktivitäten überwacht werden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.4.1; ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.40 - 2	Der Lieferant muss sicherstellen, dass Systeme des Lieferanten, auf denen Airbus-Daten gespeichert oder verarbeitet werden, oder von denen aus auf Airbus-Systeme zugegriffen wird, gegen unberechtigten Zugang geschützt sind. *Anmerkung: Auf allen Schichten wie z. B. Netzwerk (u.a. sachgemäß eingerichtete und konfigurierte Firewalls am Perimeter, eingeschränkter Internet- und WLAN-Zugriff und eingeschränkte Verbindungen zwischen Kunde/Lieferant, VPN Fernzugriff (Remote Access), Betriebssystemen und Anwendungen (einschließlich Authentifizierung und User-Management) sind adäquate Sicherheitsmechanismen erforderlich.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.1.2; ISO 27001-2013-A.9.4.1; ISO 27001-2013-A.13.1.3

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.41 - 2	Der Lieferant muss sicherstellen, dass alle Benutzer von Netzwerken und Rechnern über eindeutige, personengebundene Benutzerkennungen (User-IDs) verfügen. *Anmerkung 1: Dies gilt auch für Administrator-Accounts. Es dürfen keine gemeinsamen oder Gruppen-IDs verwendet werden, um die Vertraulichkeit von Systemen und Informationen sowie die Nachvollziehbarkeit der Benutzer und ihrer Handlungen im Netz sicherzustellen.* *Anmerkung 2: Servicekonten, die von Systemprozessen und für Maschine-zu-Maschine-Kommunikation verwendet werden, haben einen eindeutigen Owner und werden sicher gemanagt, z. B. durch die Einschränkung des interaktiven Log-ons, einer hohen Passwortkomplexität und Ablaufregeln.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.42 - 2	Der Lieferant muss sicherstellen, dass Administratoren über getrennte Accounts für Aktivitäten mit erhöhten Rechten und normaler Verwendung (IT, OT bzw. IoT), die keine höheren Zugriffsrechte erfordern (inkl. Internet- und E-Mail-Nutzung), verfügen, um zu verhindern, dass bösartiger Code unter den höheren Rechten heruntergeladen und ausgeführt wird. *Anmerkung: Die nicht privilegierten Konten sind wie für die anderen normalen Supplier-User nach dem "Prinzip der geringsten Rechte" konfiguriert.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.43 - 2	Der Lieferant muss sicherstellen, dass jeder Zugang zu Systemen und Informationen durch die Verwendung sicherer Passwörter und entsprechender User-IDs kontrolliert werden (gemäß dem Stand der Technik). *Anmerkung: Diese können durch personalisierte digitale Zertifikate gemäß vereinbarter internationaler Normen ersetzt werden.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.2.1

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.44 - 2	Der Lieferant muss Airbus-Informationen so von seinen eigenen Informationen und denen anderer Kunden trennen, dass nur autorisierte Mitarbeiter Zugang zu Airbus-Informationen erhalten können. *Anmerkung: Der Lieferant verwendet nicht dieselben physischen Arbeitsbereiche , IT-, OT bzw. IoT-Systeme oder Anwendungen ohne Rücksprache mit der Airbus-Sicherheitsabteilung für Airbus und Wettbewerber von Airbus.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.45 - 1	Der Lieferant darf ohne vorherige schriftliche Zustimmung durch Airbus anderen Firmen keinen Zugang zu Airbus-Informationen bzw. -Systemen geben.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

2.8 Anforderungen - Kryptographie

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.46 - 2	Der Lieferant muss auf Anforderung von Airbus mit den von Airbus verwendeten Standards kompatible kryptographische Tools (wie Verschlüsselung, digitale Signatur) einsetzen (Interoperabilität), um die Vertraulichkeit und Integrität sowie den Kommunikationsnachweis von transferierten und/oder gespeicherten Daten zu gewährleisten.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.10.1.1
ABR.SEC.A1015.0.47 - 1	Für Projekte/Programme, die einer militärischen, staatlichen, NATO oder OCCAR-Einstufung unterliegen, muss der Lieferant aus Gründen der Übereinstimmung und Interoperabilität die gleichen kryptographischen Tools verwenden wie Airbus. *Anmerkung: Wenn von Kunden oder Behörden gefordert, kann Airbus im Rahmen bestimmter Programme/Projekte gezwungen sein, spezielle kryptographische Tools zu verwenden.*	Lieferant von Airbus für beliebige Güter oder Dienstleistungen, die einer militärischen, staatlichen, NATO oder OCCAR Einstufung unterliegen	Airbus-intern
ABR.SEC.A1015.0.48 - 2	Falls geltendes Recht die Verwendung von Kryptographie einschränkt, muss der Lieferant auf Einzelfallbasis alternative angemessene Schutzmechanismen für Informationen beurteilen und mit Airbus vereinbaren.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.18.1.5

2.9 Anforderungen - Physische und umgebungsbezogene Sicherheit

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.49 - 2	Der Lieferant muss sicherstellen, dass der Zugang zu seinen Gebäuden, Büros und ICT-Anlagen kontrolliert und beschränkt ist (z. B. durch abgeschlossene Türen, Kartenlesegeräte, Einbruchmeldung und -reaktion, usw.), um die Vertraulichkeit von Informationen und den Zugang zu kritischen Systemen und Unternehmenswerten (Assets) wirkungsvoll zu schützen und den Diebstahl von Dokumenten oder Geräten zu verhindern.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.11.1.1
ABR.SEC.A1015.0.50 - 2	Der Lieferant muss außerdem den Zugang zu bestimmten Sonderbereichen beschränken: – Bereiche, in denen IT-, OT- bzw. IoT-Infrastruktur wie Server- oder Netzwerkräume untergebracht sind, – Bereiche, in denen Benutzer mit erhöhten Zugriffsrechten arbeiten, – Bereiche mit einem erhöhten Vertraulichkeitsgrad für Airbus (bei gesonderter Vereinbarung).	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.11.1.1
ABR.SEC.A1015.0.51 - 2	Der Lieferant muss sicherstellen, dass geschäftskritische IT-, OT- bzw. IoT-Anlagen des Lieferanten an einem Ort aufgestellt sind, wo sie reduzierten Umweltrisiken (z.B. durch Erdbeben, Überschwemmung, extreme Wetterbedingungen) ausgesetzt sind. Es werden angemessene Umgebungsschutzmaßnahmen ergriffen, um potenzielle physische Schäden abzumildern (z. B. Serverschränke/Schutzgitter, Kabelkanäle, Kühlungssystem, unterbrechungsfreie Stromversorgung (USV), Wassermelder, Brandmeldung/-löschung, Gefahrstoffmanagement usw.).	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.11.1.4; ISO 27001-2013-A.11.2.1
ABR.SEC.A1015.0.100 - 1	Der Lieferant muss für Papiere und Wechseldatenträger den Clean-Desk-Grundsatz anwenden sowie den der Clear Screen für Informationsverarbeitungseinrichtungen in Zusammenhang mit der Arbeit von Airbus.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

Released on 20 Feb 2018

2.10 Anforderungen - Betriebssicherheit

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.52 - 2	Der Lieferant muss sicherstellen, dass offizielle Änderungssteuerungsverfahren (Change Control) beim Lieferanten eingeführt sind, um sicherzustellen, dass alle an IT-Systemen, Betriebstechnik (OT) bzw. Internet der Dinge (IoT) und Infrastruktur vorgenommenen Änderungen (z. B. Konfigurationen, Upgrades, neue Anwendungen/Komponenten usw.) ordnungsgemäß dokumentiert, getestet und durch das Management verantwortlich für die IT-, OT- bzw. IoT-Systeme des Lieferanten und/oder seine Fachbereiche genehmigt sind.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.1.2; ISO 27001-2013-A.12.1.4
ABR.SEC.A1015.0.53 - 1	Sofern nicht an anderer Stelle im Vertrag zwischen Airbus und dem Lieferanten eine Ausnahme hierfür festgelegt ist, holt der Lieferant für jede Änderung, bei der Airbus-Systeme oder -Daten involviert sind, eine entsprechende Genehmigung der Airbus Security-Organisation ein, soweit die Bereiche Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit betroffen sein könnten.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.54 - 1	Der Lieferant muss Daten und Software regelmäßig sichern und die folgenden Grundsätze einhalten: – Sicherungen getrennt von produktiven Systemen aufbewahren, – Aufbewahrte Sicherungen mindestens mit demselben Grad physisch schützen wie die produktiven Systeme, – Die Wiederherstellung von Sicherungen regelmäßig testen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.3.1
ABR.SEC.A1015.0.55 - 2	Der Lieferant muss sicherstellen, dass wesentliche IT-Systeme, Betriebstechnik (OT) bzw. das Internet der Dinge (IoT) durch eine Herstellergarantie abgedeckt sind oder aber durch einen Support innerhalb der Organisation, sodass die Verfügbarkeit von Systemen und Informationen gewährleistet ist.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.11.2.4

Referenz	Beschreibung	Voraussetzung für die Anwendbarkeit	Ursprung
ABR.SEC.A1015.0.56 - 2	Der Lieferant muss unter Einsatz aller gebotenen Sorgfalt einschließlich der Verwendung von erforderlichen Technologien auf dem neuesten Stand der Technik das Eindringen bösartiger Codes (Malicious Code) auf all seinen IT-Systemen, seiner Betriebstechnik (OT) bzw. dem Internet der Dinge (IoT) sowie auf Datenträgern und möglichen Netzwerkinfrastrukturen (d. h. Server, E-Mail Gateways usw.) verhindern, damit es nicht zu einer Datenverfälschung oder zum Verlust von Rechnerleistung kommt.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.57 - 1	Der Lieferant muss sicherstellen, dass Patterns/Signaturen von Eindring- und/oder Virenschutzmechanismen auf allen Geräten - einschließlich der mobilen Geräte - regelmäßig aktualisiert werden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.58 - 1	Der Lieferant muss sicherstellen, dass kritische Patches entsprechend der Empfehlung der Softwarehersteller auf die Systeme aufgespielt werden, nachdem sie vom Lieferanten auf Kompatibilität mit seinen Einrichtungen getestet wurden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.12.6.1
ABR.SEC.A1015.0.59 - 1	Der Lieferant muss geeignete Mechanismen zur Verhinderung von Datenverlust einrichten, um die unbefugte Offenlegung von Airbus-Informationen zu verhindern.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

2.11 Anforderungen - Sicherheit der Kommunikation

Referenz	Beschreibung	Voraussetzung für die Anwendbarkeit	Ursprung
ABR.SEC.A1015.0.60 - 1	Der Lieferant verpflichtet sich zur Einhaltung der Airbus-Standards und -Verfahren für Datenaustausch und Netzanbindung, es sei denn es liegt eine anderslautende schriftliche Zustimmung von Airbus vor.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.13.2.1
ABR.SEC.A1015.0.61 - 1	Sollen Airbus-Daten durch Datennetzwerke übertragen werden, die nicht der unmittelbaren Kontrolle des Lieferanten unterliegen (z.B. Standleitungen, Internet), so muss der Lieferant alle geeigneten Maßnahmen ergreifen, um sowohl die Vertraulichkeit als auch die Integrität der Daten auf dem Übertragungsweg sicherzustellen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.13.2.2; ISO 27001-2013-A.13.1.1

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.62 - 2	Der Lieferant muss sicherstellen, dass der Datenverkehr aus dem und in das Internet oder einem anderem nicht vertrauenswürdigen Netzwerk (z.B. Testumgebungen, Netzwerke von Partnern) unter Verwendung robuster Sicherheitsmechanismen beschränkt und im Hinblick auf Auffälligkeiten überwacht wird, z.B. mittels Proxies und Gateways. *Anmerkung 1: Internetadressen, die für Missbrauchsrisiken oder als Verursacher von Angriffen bekannt sind, werden geblockt. Gleiches gilt für potenziell gefährliche E-Mails wie Spams, Phishing und verdächtige angehängte Dateien. Anmerkung 2: Der Lieferant hindert die Benutzer ebenfalls daran, solche Kontrollmechanismen zu umgehen (z.B. Benutzer, die auf alternative Proxies tunneln, Webmail oder persönliche Cloud-Dienste verwenden, um Geschäftsdaten auszutauschen, oder auch nicht autorisiertes Material herunterladen).*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.13.2.3
ABR.SEC.A1015.0.63 - 2	Der Lieferant darf nur Gerät verwenden, das von Airbus für den Anschluss an Airbus-Netzwerke, -Systeme bzw. Airbus-Produkte zugelassen worden ist (mit Ausnahme von "Lieferanten-Portalen"). *Anmerkung: Die Überwachung und das Fahren von Patches durch Airbus ist auf Geräten im Airbus-Netzwerk möglich (inkl. Updates von Anti-Schadsoftware). Eigene Geräte des Lieferanten, die diese Forderung nicht erfüllen, dürfen nur an Netzwerke angeschlossen werden, die vom Airbus-Netz getrennt sind.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.13.1.3

2.12 Anforderungen - Anschaffung, Entwicklung und Instandhaltung von Systemen

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.64 - 2	Der Lieferant muss sicherstellen, dass Produkte, die vom ihm an Airbus geliefert werden und die IT-, Betriebstechnik- (OT) oder IoT-Bestandteile enthalten (dazu zählen u.a. Softwareanwendungen, Fertigungsmittel mit integrierten Rechnern, Steuerungs- und Gebäudeleittechnik) anhand einer strukturierten und genehmigten Systementwicklungsmethode entwickelt werden, die sicherstellt, dass die Informationssicherheitsanforderungen als Bestandteil des Prozesses erachtet werden und entsprechend definiert, dokumentiert und eingehalten werden, und zwar durch Anwendung sicherer Kodierregeln und Überprüfung in der Test- und Abnahmephase.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.14.2.1
ABR.SEC.A1015.0.65 - 2	Für den Fall, dass die vom Lieferanten an Airbus gelieferten Produkte in der IT-, OT- bzw. IoT-Umgebung von Airbus eingebaut bzw. daran angeschlossen werden, muss der Lieferant sicherstellen, dass die von ihm an Airbus gelieferten Produkte in die Netzwerksicherheitsverfahren von Airbus wie Anti-Schadsoftware, Schwachstellenmanagement, Patchen, Zugriffskontrolle, Überwachung von Vorfällen und Protokollierung integrierbar sind. *Anmerkung: Zu den Produkten, die vom Lieferanten an Airbus geliefert werden und die IT , OT- oder IoT-Bestandteile enthalten, zählen u.a. Softwareanwendungen, Fertigungsmittel mit integrierten Rechnern, Steuerungs- und Gebäudeleittechnik.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.66 - 2	Der Lieferant muss sicherstellen, dass die vom Lieferanten für an Airbus gelieferte Produkte bereitgestellte Fernwartung und -betreuung mit den Airbus-Standards für Fernverbindungen konform sind. *Anmerkung: Zu den Produkten, die vom Lieferanten an Airbus geliefert werden und die IT , OT- oder IoT-Bestandteile enthalten, zählen u.a. Softwareanwendungen, Fertigungsmittel mit integrierten Rechnern, Steuerungs- und Gebäudeleittechnik.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.9.1.2

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.99 - 1	Für den Fall, dass der Lieferant sein eigenes IT-, OT- oder IoT-Gerät an seine eigenen Produkte in der Airbus-Fertigung bzw. in ein Airbus-Produkt (Flugzeug, Hubschrauber, Satellit, Drohne, usw.) eingebautes Produkt zum Zweck der Konfiguration, des Ladens von Software/ Daten, Testens oder der Fehlersuche in der Fertigungs-, Ausliefe-rungs- oder Instandhaltungsumgebung von Airbus anschließen muss, muss er sicherstellen, dass diese IT-, OT- bzw. IoT-Geräte sowie die darin enthaltene Software folgende Voraussetzungen erfüllen: – Sie sind fest zugewiesen und auf diese Art von Aktivität beschränkt und ihre Verwendung unterliegt formalen Verfahrensweisen, – sie sind während des Betriebs am Airbus-Produkt nicht an ein anderes Netzwerk als das produktinterne Netzwerk angeschlossen, – sie sind authentisch, unversehrt/ fehlerfrei und frei von Schadsoftware; dies gilt gleichermaßen für an das Gerät angeschlossene Wechseldatenträger.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

2.13 Anforderungen - Lieferantenbeziehungen

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.67 - 2	Für den Fall, dass der Lieferant einem seiner Lieferanten und/oder Unterauftragnehmer Zugang zu Airbus-Informationen geben muss, müssen alle hierin enthaltenen Anforderungen durch gesonderte Vereinbarung an den Lieferanten und/oder Unterauftragnehmer der untergeordneten Ebene weitergegeben werden. *Anmerkung 1: Der Lieferant ist allein verantwortlich für die Umsetzung von Airbus-Sicherheitsanforderungen innerhalb seiner eigenen Lieferkette.* *Anmerkung 2: Neben den industriellen Aktivitäten gilt diese Anforderung auch für Outsourcing-/Cloudprovider für die IT-, OT- bzw. IoT-Geräte des Lieferanten, für das Facility Management sowie ähnliche Dienstleistungen mit Zugang zu Airbus-Informationen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.68 - 2	Der Lieferant muss Airbus die Vereinbarung bezüglich Sicherheitsanforderungen zwischen dem Lieferanten und einem nachgeordneten Lieferanten und/oder Unterauftragnehmer auf Anfrage vorlegen. *Anmerkung: Dabei darf eine solche Vereinbarung unter keinen Umständen ein unmittelbares Vertragsverhältnis zwischen Airbus und den Lieferanten und/oder Unterauftragnehmern des Lieferanten herstellen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.69 - 2	Der Lieferant muss Sicherheits- und IS-Risiko-Überprüfungen durchführen, um zu prüfen, ob die Einhaltung dieser Directive durch den Unterauftragnehmer gewährleistet ist. *Anmerkung 1: Der Lieferant ist weiterhin für die Rückmeldung festgestellter Nichteinhaltungen an die Airbus Security-Organisation verantwortlich.* *Anmerkung 2: Airbus behält sich des Weiteren das Recht vor, die Lieferanten und/oder Unterauftragnehmer seines Lieferanten in Bezug auf diese Direktive zu bewerten; diese Bewertung kann durch Airbus Security oder einen vereinbarten unabhängigen Auditor erfolgen.* *Anmerkung 3: Der Lieferant ist befugt, einen vereinbarten unabhängigen Auditor für diese Aufgabe zu benennen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.2.1

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.70 - 2	Der Lieferant darf unter keinen Umständen einem seiner Lieferanten und/oder Unterauftragnehmer ohne vorherige schriftliche Genehmigung von Airbus Zugang zu Airbus-Daten oder -Systemen (einschließlich aber nicht beschränkt auf Routing oder Relaying) gewähren.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

2.14 Anforderungen - Handhabung von Informationssicherheitsvorfällen

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.71 - 1	Der Lieferant nimmt eine durchgängige Überwachung der Systeme und Netzwerke vor, verwendet Eindringmelde- und -schutzsysteme (Intrusion Detection/ Prevention) und protokolliert Sicherheitsvorfälle.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.72 - 1	Der Lieferant muss angemessene Maßnahmen eingerichtet haben, um hochkomplizierte Cyber-Attacken wie Advanced Persistent Threats (APT) und Command & Control Channels zu identifizieren und zu bekämpfen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.73 - 2	Der Lieferant muss einen umfassenden und genehmigten Vorfall-Management-Prozess für Informationen und Systeme etablieren, der die Identifizierung, Reaktion und Behebung von Informationssicherheitsvor-fällen, ein Berichtswesen und eine Beweissicherung sowie eine Überprüfung von Maßnahmen nach deren Einführung beinhaltet. *Anmerkung: Zu den Vorfällen zählen u.a. verloren gegangene oder gestohlene Geräte, Fehlfunktionen, Stromausfall, Überlasten, Fehler durch Benutzer/IT-, OT- oder IoT-Mitarbeiter, Zugriffsverletzungen, Schadsoftware und Hacking.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.16.1.1
ABR.SEC.A1015.0.74 - 2	Der Lieferant muss Sicherheitsschwachstellen und -vorfälle identifizieren und klären, ihre Auswirkungen auf das Unternehmen minimieren und das Risiko verringern, dass ähnliche Sicherheitsvorfälle wiederholt auftreten.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.16.1.1

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.75 - 2	Für den Fall, dass Sicherheitsvorfälle eintreten, die Airbus-Systeme oder -Informationen möglicherweise betreffen, muss der Lieferant eine Untersuchung durchführen und den Vorfall unverzüglich und ohne Aufforderung gegenüber der Airbus Security melden. *Anmerkung: Zu solchen Vorfällen zählen u.a.: Diebstahl von Geräten, auf denen Airbus-Informationen gespeichert sind, Lecks von Airbus-Daten aus Systemen des Lieferanten, Kompromittierung von Systemen, die mit Airbus verbunden sind.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.2.1; ISO 27001-2013-A.16.1.2
ABR.SEC.A1015.0.76 - 2	Der Lieferant muss Abhilfemaßnahmen in Bezug auf festgestellte oder gemeldete Sicherheitsvorfälle durchführen. *Anmerkung: Sollte Airbus in seinen Systemen beliebige Arten von Sicherheitsvorfällen vorfinden, die vom Lieferanten herrühren, benachrichtigt Airbus den Lieferanten unverzüglich und behält sich das Recht vor, die Konnektivität mit dem Lieferanten vorübergehend auszusetzen oder einzuschränken.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.16.1.5

2.15 Anforderungen - Informationssicherheitsaspekte bei der Aufrechterhaltung des Geschäftsbetriebs (Business Continuity)

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.77 - 2	Der Lieferant muss für den Fall eines größeren Ausfalls oder höherer Gewalt einen Notfallvorsorgeplan/Plan zur Aufrechterhaltung des Geschäftsbetriebs für die Aufrechterhaltung/Wiederherstellung der IT-, OT- bzw. IoT-Dienste erstellt haben (einschließlich aber nicht beschränkt auf: physische Beschädigungen, Unterbrechungen der Stromversorgung, Feuer, Naturkatastrophe). *Anmerkung: Ein solches Programm besteht aus Management-Framework, Notfallvorsorgeplänen, Pflege, Überprüfung & Tests sowie Wiederaufnahme des Geschäftsbetriebs und K-Fall-Plänen.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.17.1.1

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.78 - 1	Management-Framework - Der Lieferant muss geeignete Mechanismen, Abläufe, festgelegte Rollen und Verantwortlichkeiten eingerichtet haben, um die Kontinuität der Geschäftsprozesse zu gewährleisten und größere Unterbrechungen zu vermeiden. *Anmerkung: Dies soll folgendes umfassen: Risikoidentifizierung und -bewertung, Risikominderungsstrategien, Aufrechterhaltung der Verfügbarkeit der Dienste, Prozesse und Produkte des Unternehmens durch Sensibilisierung, Reviews und Tests.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.17.1.1
ABR.SEC.A1015.0.79 - 1	Notfallvorsorgepläne - Der Lieferant dokumentiert seine Notfallvorsorgepläne und schult seine Mitarbeiter entsprechend, um sicherzustellen, dass der Geschäftsbetrieb im Falle eines größeren Vorfalls auf einem zuverlässigen Niveau aufrechterhalten wird.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.17.1.2
ABR.SEC.A1015.0.80 - 1	Pflege, Überprüfung, Tests - Der Lieferant muss in der Lage sein nachzuweisen, dass die Pläne regelmäßig überprüft und gepflegt sowie durch Übungen getestet werden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.17.1.3
ABR.SEC.A1015.0.81 - 2	Wiederaufnahme des Geschäftsbetriebs und K-Fall-Pläne - Der Lieferant muss für seine mit Airbus in Verbindung stehenden Geschäftstätigkeiten und internen abhängigen Systeme und Prozesse einen K-Fall-Plan erstellen. *Anmerkung: Dieser umfasst die Planung sowie die einzelnen Schritte, die während oder nach einem Vorfall eingeleitet werden müssen, sodass die Geschäftstätigkeiten wieder auf normalem Niveau aufgenommen werden können.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.17.1.2

2.16 Anforderungen - Compliance (Richtlinienkonformität)

Sowohl Airbus als auch der Lieferant verpflichten sich, die entsprechenden gesetzlichen Bestimmungen einzuhalten (insbesondere wenn es sich um eine internationale Zugangsregelung handelt, die mehrere unterschiedliche Zuständigkeiten/Gerichtsbarkeiten umfasst). Für unterschiedliche Lieferanten wird es auch unterschiedliche Zuständigkeiten geben, so dass hier von Fall zu Fall geprüft werden muss.

Hierbei ist besonderes Augenmerk auf Gesetzeskollisionen zu legen, insbesondere hinsichtlich personenbezogenem Datenschutz, Überwachung, Aufbewahrung von Daten und Kryptographie.

Der Lieferant erkennt an, dass die Airbus-Security-Organisation bzw. ein unabhängiger von Airbus benannter Auditor die Sicherheit der Systeme, Prozesse und Abläufe des Lieferanten überprüfen darf, in die Airbus-Systeme oder -Informationen eingestellt werden oder von denen aus auf sie zugegriffen wird.

Airbus behält sich das Recht vor, unter angemessener Vorankündigung nach eigenem Ermessen Audits der Einhaltung und/oder Umsetzung von Maßnahmen durchzuführen.

Airbus behält sich das Recht vor, die Konnektivität bzw. den Zugang zu Informationen für den Lieferanten zu beenden bzw. einzuschränken, wenn bei einem Audit der Zugang verwehrt wird, Korrekturmaßnahmen nicht umgesetzt werden oder eine ungenügende Mitwirkung im Falle eines schwerwiegenden Sicherheitsvorfalls besteht.

Im Falle einer wesentlichen Änderung der Verhältnisse des Lieferanten (einschließlich, jedoch nicht beschränkt auf Fusionen, Übernahmen oder andere Umstrukturierungen des Unternehmens) oder seiner Geschäftstätigkeiten behält sich Airbus das Recht vor, die Übereinstimmung des Lieferanten mit den für den Schutz von Informationen und Infrastruktur erforderlichen Sicherheitsanforderungen in Zusammenhang mit Airbus erneut zu beurteilen.

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.82 - 1	Der Lieferant muss regelmäßige Überprüfungen und Audits im Hinblick auf die folgenden Punkte sicherstellen: – die technische Robustheit der Systeme, – die Einhaltung der Grundsätze (Policy), – Verfahrensabläufe für den Schutz von Systemen und Informationen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.18.2.1
ABR.SEC.A1015.0.83 - 1	Der Lieferant muss alle maßgeblichen Gesetze und Vorschriften bezüglich geistigen Eigentums und Urheberrechten einhalten und alle erforderlichen Software-Lizenzen erwerben.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.18.1.2
ABR.SEC.A1015.0.84 - 2	Der Lieferant muss Airbus (oder einem vereinbarten unabhängigen Auditor) Zugang zu Gebäuden, Unterlagen, Systemen usw. zum Zwecke der Prüfung und Validierung der Sicherheitsregelungen in Übereinstimmung mit dieser Direktive und für die generelle Minderung des ICT-Risikos gewähren. *Anmerkung: Ein solcher Zugang kann auch in die Lieferkette des Lieferanten heruntergebrochen werden, wenn davon ausgegangen wird, dass ein Datenaustausch oder eine Systemanbindung an Airbus-Systeme erfolgt.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.2.1

Referenz	Beschreibung	Voraussetzung für die Anwendbarkeit	Ursprung
ABR.SEC.A1015.0.85 - 1	Der Lieferant ist verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um Airbus die für eine Sicherheitsbewertung durch Airbus selbst oder einen unabhängigen Auditor erforderlichen Informationen bereitzustellen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.15.2.1
ABR.SEC.A1015.0.86 - 1	Der Lieferant muss geeignete Abhilfemaßnahmen in Bezug auf sämtliche Mängel, die durch das Audit festgestellt wurden, einleiten.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.88 - 2	Der Lieferant muss in der Lage sein, Airbus einen Nachweis darüber vorzulegen, dass seine Organisation die maßgeblichen Exportgesetze und -vorschriften erfüllt und dass sie die Nachvollziehbarkeit dessen gewährleistet, sodass der Lieferant bei Kontrollen seinen Nachweispflichten nachkommen kann. *Anmerkung: Airbus darf zu jeder Zeit die Zuverlässigkeit der Organisation des Lieferanten im Hinblick auf diese Anforderungen überprüfen (physisch und logisch). Hierzu zählt u.a. die Sicherstellung der Identität und Nationalität(en) von Benutzern, Zugangsberechtigungsvergaben und Zugangsgenehmigungs- und -kontrollmechanismen (einschließlich eines offiziellen Benutzer-Akkreditierungsverfahrens), die Kontrolle des Informationsflusses sowie Zugriffsprotokolle.*	Lieferant - Lieferant von Airbus für beliebige Güter, technische Daten oder Dienstleistungen, die den Exportkontrollgesetzen und -vorschriften unterliegen.	Airbus-intern
ABR.SEC.A1015.0.90 - 2	Wenn die vertragliche Beziehung es erfordert, dass der Lieferant Zugang zu Informationen erhält, die einem staatlichen, NATO- oder OCCAR-Geheimschutz unterliegen, muss der Lieferant alle technischen und organisatorischen Mittel einsetzen, um den nationalen Geheimhaltungsregularien des Landes, in dem er seinen Vertrag ausführt, erfüllt, und zwar gemäß den von Airbus in den entsprechenden Programmsicherheitsanweisungen (Programme Security Instructions) bzw. Sicherheitsvorgaben (Security Aspect Letters) angegebenen Einstufungsgraden.	Lieferant - Lieferant von Airbus für beliebige Güter, technische Daten oder Dienstleistungen, die einer militärischen, staatlichen, NATO oder OCCAR Einstufung unterliegen	Airbus-intern

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.91 - 1	Der Lieferant muss Airbus im Falle von Vorladungen, Ermittlungen o. Ä., bei denen Airbus-Informationen angefordert werden, entsprechende Informationen zur Verfügung stellen und mit Airbus kooperieren. Der Lieferant muss Airbus auch im Rahmen von Zertifizierungs-/Zulassungsprozessen o. Ä., für die Airbus-Informationen - einschließlich der sich im Besitz des Lieferanten befindlichen Informationen - erforderlich sind, unterstützen und entsprechende Informationen zur Verfügung stellen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.92 - 2	Der Lieferant muss Airbus bei Erhalt einer Aufforderung zur Herausgabe von Airbus-Informationen an andere Dritte, einschließlich öffentlicher Verwaltungen oder Behörden, unverzüglich informieren. *Anmerkung: Der Lieferant schöpft alle rechtlichen Mittel aus, um sich derartigen Zugriffsersuchen zu widersetzen, es sei denn, sie wurden durch Airbus genehmigt.*	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern

2.17 Anforderungen - Kündigung/Beendigung

Referenz	*Beschreibung*	*Voraussetzung für die Anwendbarkeit*	*Ursprung*
ABR.SEC.A1015.0.93 - 1	Bei oder vor der Vertragsunterzeichnung muss der Lieferant Airbus einen Plan für das Ende des Vertrages vorlegen, der aufzeigt, wie Airbus-Informationen - einschließlich unterstützender und Archiv-Informationen - zum Ende dieser Vereinbarung an Airbus zurückgegeben werden, und wie alle Airbus-Informationen dauerhaft von den Geräten und Einrichtungen des Lieferanten entfernt werden.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.94 - 1	Der Lieferant muss den Schutz der Airbus-Informationen und -Systeme sicherstellen, einschließlich der Fortführung des Services bei Ablauf der vereinbarten Vertragsdauer/ vertraglichen Vereinbarungen und der Einhaltung der vertraglich festgelegten Bestimmungen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	Airbus-intern
ABR.SEC.A1015.0.95 - 1	Der Lieferant muss Airbus umgehend in Kenntnis setzen, wenn er den Zugang zu bestimmten oder allen Airbus-Daten oder -Systemen nicht länger benötigt, um seinen Verpflichtungen im Rahmen des Vertrags bzw. der vertraglichen Vereinbarungen nachzukommen.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.1.4

Referenz	***Beschreibung***	***Voraussetzung für die Anwendbarkeit***	***Ursprung***
ABR.SEC.A1015.0.96 - 1	Nach Ablauf der für die Verwendung der Informationen vereinbarten Frist oder zu einem Zeitpunkt, wenn die Informationen nicht mehr benötigt werden, müssen sie wie mit Airbus vereinbart durch den Lieferanten entsorgt werden, wobei sicherzustellen ist, dass sie nicht wiederhergestellt werden können.	Lieferant - Lieferant von Airbus für beliebige Güter oder Dienstleistungen	ISO 27001-2013-A.8.1.4

3 Bezugsunterlagen

Die nachstehend aufgeführten Dokumente wurden bei der Erstellung dieser Direktive herangezogen. Sie sind jedoch nicht als integraler Bestandteil des Vertrags/der vertraglichen Vereinbarung zwischen Airbus und dem Lieferanten auf der Grundlage dieser Direktive zu erachten, es sei denn dies ist eindeutig in der entsprechenden Anforderung angegeben und festgelegt. Auf Anfrage stellt Airbus dem Lieferanten die Bezugsunterlagen zur Verfügung.

HINWEIS: Jegliche ISO- oder ISF-Dokumente müssen unmittelbar durch den Lieferanten beschafft werden, da Airbus solche Dokumente aus Urheberrechtsgründen nicht bereitstellen kann.

Dok. Referenz	***Titel***
A1044	Security Requirements for Classification & Protection of Information *(Sicherheitsanforderungen für die Einstufung und den Schutz von Informationen)*
GTC	General Terms and Conditions for Access to and Use of Airbus Supplier Portals *(Allgemeine Geschäftsbedingungen für den Zugriff auf und die Verwendung von Airbus-Lieferantenportalen)*
ICT/IST Charter	Airbus Information Management - Verwendung von IST Facilities
ISO/IEC 27001	Information technology - Information security management systems - Requirements *(Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen)*
ISO/IEC 27002	Information Technology - Security techniques - Code of practice for information security controls *(Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen)*
ISO/IEC 27003	Information technology - Security techniques - Information Security *(Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits)*
ISO/IEC 27036	Information technology - Security techniques - Information security for supplier relationships management system implementation guidance *(Umsetzungsleitfaden für das Management von Lieferantenbeziehungen bzw. Informationstechnik - Sicherheitsverfahren - Informationssicherheit)*
IEC 62443 Teil 2-1 2010	Industrial communication networks - Network and system security - Establishing an industrial automation and control system security program *(Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Einrichten eines IT-Sicherheitprogramms für industrielle Automatisierungssysteme)*
SoGP April 2016	The ISF Standard of Good Practice in Information Security *(ISF-Standard für Good Practice in der Informationssicherheit)*

4 Glossar

maßgeblich LEXINET

Airbus	Bezeichnet Airbus S.A.S. und ihre Tochtergesellschaften, Konzerngesellschaften, Joint Ventures und verbundene Unternehmen
Airbus-Informationen	Im Kontext dieser Direktive bezeichnet der Begriff die Rechte von Airbus an geistigem Eigentum, Verfahren, Fachwissen, geschützten und/oder vertraulichen Technologien und Prozessen, internen Fakten und Zahlen sowie alle damit zusammenhängenden Materialien und Dokumente. Dies umfasst auch alle möglichen Mittel und Verfahren für die Speicherung und Übertragung in jeglichem Format oder auf jeglichem Medium (einschließlich aber nicht beschränkt auf Papierdokumente, Ausdrucke, Mikrofiches, elektronische Daten in beliebiger Form, Bilder und Multimedia)
Airbus-Sicherheit	Bezeichnet im Kontext dieser Direktive die Organisation und die Mitarbeiter bei Airbus, die dafür verantwortlich sind, die Airbus-Mitarbeiter, Informationen/Daten, Tätigkeiten, das wissenschaftliche und technische Erbe sowie Unternehmenswerte und -Image gegen alle feindlichen Handlungen zu schützen, und zwar so, dass solche feindlichen Handlungen verhindert und festgestellt werden und auf sie reagiert wird
Sicherstellung des Geschäftsbetriebs (Business Continuity)	Steht im Kontext dieser Direktive für die strategische und taktische Fähigkeit des Betriebs des Lieferanten, für den Fall von Vorfällen und Unterbrechungen des Geschäftsbetriebs vorauszuplanen und auf diese zu reagieren, um den Geschäftsbetrieb auf einem für die Gewährleistung der Vertragserfüllung annehmbaren Niveau fortzuführen
Cyber	Im Kontext dieser Direktive ist die dynamische, stets mit dem Netz verbundene ("online") und technologisch vernetzte Welt gemeint; sie besteht aus Menschen, Organisationen, Informationen und Technik. Sie verändert sich ständig auf unvorhersehbare Weise, erleichtert die Zusammenarbeit aber vermindert das Risiko zur Durchführung krimineller Aktivitäten, bündelt Ziele und versteckt die Täter
Daten	Im Kontext dieser Direktive steht der Begriff für sämtliche Informationen in elektronischer Form in jeglichem Format und auf jeglichem Medium
Informations-sicherheit	Steht für den Schutz von: – Verfügbarkeit - Zur Verhinderung des Verlustes von Informationen und Diensten, z.B. durch bösartige Codes, Naturkatastrophen, Systemausfälle/-störungen – Unversehrtheit - Zur Verhinderung unbefugter Eingabe, Änderung, Verarbeitung oder Löschung. – Vertraulichkeit - Zur Verhinderung unbefugter Offenlegung. – Nachvollziehbarkeit/Rechenschaftspflicht - Zur Sicherstellung der User-Identität und der individuellen Verantwortlichkeit sowie Audit-Trails (Prozesshistorien) für den Zugang und für Transaktionen zur Verhinderung und Erkennung betrügerischen Eindringens

Informations-technologie oder IT	Steht im Kontext dieser Direktive für jegliche Informationstechnik- oder Telekommunikationsgeräte bzw. Dienstleistungen, Software und zugehörige Prozesse für die Speicherung, Verarbeitung und Übertragung von Daten. Damit gemeint unter anderem PCs, Workstations, Laptops, Wechseldatenträger, Telefone, Smartphones, Netzwerke, Systeme, Computerprogramme, Server, Datenbanken und -Webportale
ISF	Information Security Forum
ISMS	Information Security Management System
NATO	North Atlantic Treaty Organization
OCCAR	Organisation Conjointe de Coopération en matière d'Armement
Operational Technology oder OT (Betriebstechnik)	Steht im Kontext dieser Direktive für jegliche Datenmanagement- bzw. Kommunikationstechnik- oder Telekommunikationsgeräte bzw. Dienstleistungen, Firmware-Software und zugehörige Prozesse für die Speicherung, Verarbeitung und Übertragung von Daten, die in betriebstechnische Geräte (OT) eingebettet ist. Damit gemeint sind u.a. Mensch-Maschine-Schnittstellen, Front End Interface, Wechseldatenträger, Netzwerke, in der Fertigung verwendete SPS-Steuerungen und Gebäudeleittechnik
Risiko	Steht im Kontext dieser Direktive für ein Ereignis oder einen Zustand, das/der - wenn es/er eintritt - negative Auswirkungen auf Ziele und Vertragserfüllung des Lieferanten hat, und zwar hinsichtlich Konstruktion, Produktion und/oder der zukünftigen Lieferung von Produkten/Dienstleistungen an Airbus
Risikomanagement	Bezeichnet einen vorausschauenden Managementprozess, der mögliche Risiken in Bezug auf die Unternehmensziele des Lieferanten sowie ihre Minderung vorwegnimmt, so dass Informationssysteme an sich (oder die entsprechenden Unternehmensprozesse, die sie unterstützen) nicht unmittelbar von den Folgen bedroht werden, die vernünftigerweise vorhergesehen und umgangen hätten werden sollen
Lieferant	Bezeichnet im Kontext dieser Direktive die Einheiten, die zugunsten von Airbus Erzeugnisse und/oder Leistungen bereitstellen, und nicht Teil von Airbus sind (einschließlich aber nicht beschränkt auf Lieferanten, Unterauftragnehmer, Dienstleister, industrielle Partner und Forschungszentren)
Internet of Things oder IoT (Internet der Dinge)	Steht im Kontext dieser Direktive für das Netz aus physischen Geräten, Fahrzeugen und anderen Komponenten mit integrierter Elektronik, Software, Sensoren, Stellantrieben und Netzanbindung, welche es ihnen ermöglicht, Daten zu erfassen und auszutauschen. Jedes "Ding" ist eindeutig anhand seines eingebauten Rechensystems identifizierbar, kann aber innerhalb der bestehenden Internet-Infrastruktur verwendet werden

Mitwirkende

Name	*Funktion*
ALTSTÄDT Kai	Prod. Indust & Operational Security MGR - EIDS
BALLARD Florence	Security Business Partners - ZSB
BOUDET Florent	Security Assurance - ZSG
DENIS Pierrette	Security Operations - ZSO
GAUVRY Philippe	Q Procurement Requirements Proj Mgr - QPR
JORDAN Marie	Prod. Secur Capabilities Compliance MGR - EIDC1
MEIER-HEDDE Felix	Prod. Indust & Operational Security MGR - EIDS
REY Nathalie	Prod. Indust & Operational Security MGR - EIDS
THORNARY Mathieu	IM Security Analyst - ZIST
TREDEZ Juliette	Governance - ZSG
UTH Fridtjof	Security Assurance - ZSG

Akzeptable Übersetzung für die Anwendung in der lokalen Sprache

Funktion	*Name*	*Datum*
Validierung Deutsche Übersetzung	**UTH Fridtjof**	**14/02/18**

Änderungsverzeichnis

Ausgabe	*Datum*	*Änderungsgrund*
A	Dez 2017	Erstausgabe. Dokument wurde vollständig überarbeitet. Verschmelzung der Airbus A1015 und der früheren Airbus Group E260, inkl. der Anforderungen von Airbus Helicopters und Airbus Defence&Space und Produkt-/ Betriebstechnikaspekten.
	Feb 2018	**Die Übersetzung in die deutsche Sprache ist verfügbar.**

Requisitos sobre Seguridad de la Información para Proveedores

OBJETIVO/ÁMBITO DE APLICACION :

Esta Directiva define los requisitos de seguridad y gestión de riesgos de la información de Airbus para Proveedores. El objetivo de esta directiva A1015.0 (en lo sucesivo, la "Directiva") es mantener la seguridad de la información empresarial de Airbus, los sistemas de procesamiento de información organizativa, los productos y las instalaciones a las que los Proveedores y sus propios Proveedores acceden o las que estos operan o procesan, ya estén situadas dentro o fuera de las sedes de Airbus.

Procurement de Airbus aplicará los requisitos de seguridad de la información de Airbus de acuerdo con lo establecido en esta Directiva, sin desviación alguna, a todos los contratos o acuerdos contractuales de Proveedores con cualquier entidad, sede o localización de Airbus, incluidas las filiales y empresas conjuntas en las que Airbus posea participaciones de control. Esta Directiva se podrá complementar con acuerdos específicos de seguridad correspondientes al trabajo contratado o producto comprado si el nivel de sensibilidad de la información o la conectividad lo requieren o si así lo exigen las normativas internas o externas.

Documento del Propietario :

Nombre : KNUEPPEL Dietrich

Función : Directive Owner

Autorizador para Aplicación :

Nombre : ANDREI Pascal

Función : SEC FoR Owner

INDICE

1 Introducción

Existe una demanda de negocio cada vez mayor para proporcionar a los Proveedores de Airbus acceso directo o integrado a la Información y a los Sistemas de información de Airbus y, por tanto, a sus datos, pero se reconoce que esto expone a Airbus a diversos riesgos. El objetivo de esta Directiva es definir cómo se exige que trabajen los Proveedores para construir una colaboración de confianza.

Airbus reconoce que, al ofrecer a los Proveedores acceso a información y a los sistemas de información, se introducen riesgos por :

- pérdida de control allí donde los Proveedores acceden o gestionan información de Airbus y sus sistemas de información,
- pérdida de control y responsabilidad cuando la información de Airbus y los sistemas de información se encuentran fuera de las sedes de Airbus,
- pérdida de visibilidad de la actividad del Proveedor respecto a las restricciones de seguridad de Airbus.

También se reconoce que una protección inadecuada de los datos y sistemas propios de los Proveedores pone en peligro tanto la calidad como la entrega en plazo de bienes y servicios a Airbus. Por tanto, la seguridad adecuada de IT, OT o IoT y la continuidad del negocio por parte del Proveedor también son un requisito desde el punto de vista industrial.

Así pues, los requisitos establecidos en esta Directiva se implementarán en cada uno de los siguientes casos :

- el Proveedor accede a los sistemas de información de Airbus, los sistemas de fabricación de Airbus o los productos de Airbus por medios de IT (de forma remota o en la sede),
- el Proveedor guarda información de Airbus,
- el Proveedor aprovecha sus propios sistemas de IT, OT o IoT para fabricar, entregar, instalar, mantener productos o prestar servicios a Airbus.

Además, la seguridad de los datos en proyectos colaborativos, así como la información interna y el intercambio de datos se encuentran bajo un escrutinio de las agencias gubernamentales de Europa y EE. UU. cada vez mayor.

El ciberespionaje representa una amenaza sustancial y creciente para las empresas que operan en ciertos sectores clave, incluida la tecnología aeroespacial y de defensa. Las ciberdefensas bien desarrolladas de Airbus ofrecen cierto grado de seguridad, pero las amenazas también pueden proceder de la cadena de suministro. Los Proveedores tienen acceso a la Información y a los sistemas de Airbus, pero pueden no contar con la infraestructura de seguridad necesaria para proteger los activos de información adecuadamente y, por tanto, correr el riesgo de incumplir de manera pasiva los Acuerdos de no divulgación.

Airbus tiene el compromiso de reflejar los requisitos de seguridad correspondientes garantizando un nivel de seguridad de la información apropiado en su cadena de suministro.

2 Requisitos

2.1 Requisitos : Acuerdo de Trabajo Colaborativo

El objetivo de Airbus es colaborar con los Proveedores conforme a normas o acuerdos respetados por todos.

Este documento es aplicable como complemento a los "Términos y condiciones generales (GTC) de acceso y uso a los portales de proveedores de Airbus".

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.1 - 2	El Proveedor se comprometerá a trabajar de manera profesional y aplicar de buena fe todos los requisitos de seguridad incluidos en este documento.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.1.2 ; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.2 - 1	El Proveedor será responsable de sus actividades operativas diarias en los sistemas y con la información de Airbus, de acuerdo con esta Directiva.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.1.2 ; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.3 - 1	El Proveedor aplicará una protección base conforme a esta Directiva antes o despues dela ejecución del Contrato/acuerdos contractuales con Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.1.2 ; ISO 27001-2013-A.7.2.1
ABR.SEC.A1015.0.4 - 2	El Proveedor será responsable de poner en marcha los procesos adecuados de Gestión de riesgos de seguridad y garantizar que sus propios subcontratistas/proveedores apliquen también estos procesos de Gestión de riesgos de seguridad en sus organizaciones. *Nota 1 : El Proveedor reevalúa periódicamente sus riesgos de seguridad para Airbus puesto que se pueden detectar nuevas vulnerabilidades, ya que el escenario de amenazas puede variar, las organizaciones cambian y la tecnología progresa.* *Nota 2 : El Proveedor mantiene un registro de riesgos de seguridad y un plan de respuesta (aceptar, mitigar, evitar o transferir y notificar a Airbus los riesgos de seguridad que puedan afectar a los servicios prestados o productos entregados).*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.5 - 2	El Proveedor solo accederá, utilizará, modificará y/o eliminará cualquier aspecto de los sistemas o datos de Airbus en la medida en que Airbus lo autorice. *Nota : El Proveedor no intentará acceder a ningún sistema o información para los que no tenga autorización de Airbus a efectos de la ejecución de un contrato.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.6 - 1	El Proveedor no intentará evitar, modificar o deshabilitar ninguna red y/o mecanismo de seguridad de los sistemas de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.1.2
ABR.SEC.A1015.0.7 - 2	El Proveedor será responsable de garantizar que no se contravenga ninguna disposición sobre seguridad de Airbus (p. ej. Política de uso aceptable/ICT Charter al trabajar en los sistemas de Airbus, Normativas de la planta para visitantes, personal de la sede, etc...), salvo que exista un acuerdo por escrito con el departamento de seguridad de Airbus. *Nota : Es posible que el Proveedor necesite una acreditación gubernamental (Facility Security Clearance) para trabajar en algunas de las sedes o proyectos de Airbus.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.11.1.5
ABR.SEC.A1015.0.97 - 1	El Proveedor protegerá contra pérdida, destrucción, falsificación, corrupción, acceso o publicación no autorizados, toda la Información relevante de Airbus a la que acceda, con la que opere o que procese. *Nota : Esta protección deberá seguir incluso tras el fin del contrato.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.2 Requisitos : Evaluación Inicial

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.8 - 2	Antes de iniciar un intercambio de datos o la conectividad con cualquier sistema o red, el Proveedor deberá proporcionar a Seguridad de Airbus toda la información y documentación necesarias para poder evaluar el nivel de seguridad del Proveedor en relación con esta Directiva. *Nota 1 : Incluye una copia de la política actual del Proveedor sobre seguridad de la información, y su política sobre la seguridad física en el acceso a lugares o dispositivos que se puedan conectar a los sistemas de Airbus o procesar Información de Airbus.* *Nota 2 : Airbus garantizará la confidencialidad de toda la información proporcionada por el Proveedor.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.1.1

2.3 Requisitos : Políticas de Seguridad

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.10 - 1	El Proveedor garantizará un compromiso de gestión formal y una concienciación eficiente del usuario mediante el desarrollo y la distribución de una política de seguridad de la información exhaustiva y aprobada y directrices de usuario a todas las personas con acceso a la información y a los sistemas.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.5.1.1
ABR.SEC.A1015.0.11 - 1	A partir de su política de seguridad de la información, el Proveedor establecerá un conjunto de criterios y procedimientos dirigidos a usuarios con privilegios (por ejemplo, administradores, programadores) para garantizar una aplicación coherente de los controles de seguridad de la información.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.5.1.1

2.4 Requisitos : Organización de la Seguridad

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.12 - 2	Nombramiento de un director de Seguridad - el Proveedor nombrará a uno de sus empleados con responsabilidad global a efectos de seguridad y cuestiones de riesgo y otorgará la autoridad adecuada y los medios a esta función para coordinar la actividad en toda la organización.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.6.1.1
ABR.SEC.A1015.0.13 - 1	El director de Seguridad tendrá constancia de todos los requisitos jurídicos y contractuales aplicables, lo cual incluye, de manera enunciativa, pero no limitativa, aquellos dispuestos en esta Directiva y de conformidad de exportación que afecten a los controles de seguridad, procesos y sistemas del Proveedor.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.18.1.1
ABR.SEC.A1015.0.14 - 2	El Proveedor nombrará en su organización a un punto de contacto para Seguridad de Airbus, que sea responsable de la colaboración rutinaria y la comunicación de incidentes.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.15 - 2	El Proveedor separará obligaciones y áreas de responsabilidad en los ámbitos de seguridad y de IT, OT o IoT para reducir el riesgo de uso incorrecto de los sistemas o aplicaciones, ya sea de manera accidental o deliberada.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.6.1.2

2.5 Requisitos : Seguridad de los Recursos Humanos

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.16 - 2	El Proveedor será el único responsable de la aplicación de los requisitos de seguridad de Airbus en su organización y, por tanto, deberá garantizar que los usuarios estén debidamente cualificados y formados.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.17 - 2	El Proveedor contará con procesos sistemáticos de verificación de personal para comprobar la identidad y los antecedentes de su personal. *Nota 1 : Esto debería incluir la verificación del título de mayor nivel obtenido, el domicilio de residencia en los últimos años, referencias de empleos anteriores, comprobación de la validez de los documentos de identidad presentados y de que no se haya cometido ningún delito grave.* *Nota 2 : En países en los que este proceso esté restringido por las leyes y normativas, el Proveedor llevará a cabo el proceso de verificación en la medida en que las leyes y normativas lo permitan.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.18 - 1	El Proveedor proporcionará, bajo petición, información de verificación de su personal. *Nota : En el caso del trabajo sujeto a normativas gubernamentales u otros proyectos confidenciales, Airbus se reserva el derecho a solicitar información de verificación de seguridad, si procede y en la medida en que la legislación lo permita.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.1.1
ABR.SEC.A1015.0.19 - 1	El Proveedor se asegurará de que todos sus empleados y proveedores/ subcontratistas que tengan acceso a Información y datos de Airbus sean conscientes de la naturaleza confidencial de esa información y las obligaciones incluidas en esta Directiva mediante actividades de formación y concienciación adecuadas.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.2.2
ABR.SEC.A1015.0.20 - 2	El Proveedor garantizará que los contratos con sus empleados y proveedores/subcontratistas cumplan los compromisos de confidencialidad establecidos en la presente Directiva.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.1.2

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.21 - 2	El Proveedor nombrará al personal responsable de la gestión y la seguridad de sus sistemas de información y notificará a Airbus sin demora de cualquier cambio en este personal. *Nota : El Proveedor se compromete a que cualquier personal de sustitución tenga un nivel de competencia equivalente.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.22 - 1	En caso de que se detecte un problema de seguridad relativo a un empleado de algún Proveedor, Airbus notificará al Proveedor su desaprobación en cuanto a la asignación de dicho empleado al trabajo de Airbus. En este caso, el Proveedor tomará todas las medidas necesarias para garantizar que este empleado no tenga acceso a activos registrados o confidenciales facilitados al Proveedor en relación con su trabajo para Airbus. *Nota : Los activos mencionados anteriormente incluyen, entre otros, documentos y datos, cualquier sistema de información (hardware y software) o productos físicos.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.7.2.3

2.6 Requisitos : Gestión de Activos

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.23 - 2	El Proveedor considerará toda la Información que se transfiera entre el Proveedor y Airbus como "Airbus internal" o "Documento interno de Airbus" (véase "A1044 - Protección y clasificación de la información" *(A1044 - "Protection and Classification of Information"))*. *Nota : El acceso a información clasificada de niveles superiores estará sujeto a un acuerdo específico.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.13.2.2 ; ISO 27001-2013-A.8.2.1 ; ISO 27001-2013-A.8.2.2
ABR.SEC.A1015.0.24 - 1	El Proveedor aplicará procedimientos de gestión de la información en relación con los niveles de clasificación de Airbus (véase A1044 - "Directiva de protección y clasificación de la información" (*A1044 - "Protection and Classification of Information"*)), promoverá la concienciación y garantizará el cumplimiento por parte de sus usuarios.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.2.3

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.25 - 2	El Proveedor mantendrá una lista actualizada de los equipos de IT, OT e IoT autorizados que utiliza para acceder, transferir, procesar y/o almacenar Información de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.26 - 1	Bajo petición, el Proveedor proporcionará a Airbus una lista de todos los sistemas y dispositivos en los que se almacene o procese Información de Airbus (en concreto, localización física, localización en la red y objetivo empresarial del almacenamiento/procesamiento).	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.27 - 1	En caso de que el proveedor cuente con la certificación ISO27001, añadirá la Información de Airbus y la conectividad con Airbus al inventario de activos ISMS.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.1.1
ABR.SEC.A1015.0.28 - 2	El Proveedor no almacenará información de Airbus en dispositivos móviles (teléfonos inteligentes, portátiles, memorias USB, etc...) salvo que esté encriptada con productos/criterios de avanzada tecnología.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.1.3
ABR.SEC.A1015.0.29 - 1	Cualquier medio utilizado o roto que contenga Información de Airbus será borrado o destruido de manera efectiva antes de que sea retirado o reutilizado.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.3.2

2.7 Requisitos : Control de Acceso

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.30 - 2	El Proveedor solo utilizará métodos y controles de acceso permitidos proporcionados o exigidos por Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.1.1
ABR.SEC.A1015.0.31 - 1	El Proveedor identificará y registrará debidamente las conexiones en las redes y sistemas de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.32 - 1	El Proveedor mantendrá un diagrama de red lógico que incluya las conexiones externas y detalle específicamente la conexión a Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.33 - 2	El Proveedor mantendrá una lista actualizada con las autorizaciones de usuarios en los sistemas de su organización.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.34 - 2	El Proveedor garantizará que el proceso de solicitud y autorización del usuario en relación con los derechos de acceso a sus propios sistemas y a los sistemas de Airbus sea rastreable en su organización y cumpla el principio de "necesidad de saber".	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.35 - 1	El Proveedor revocará, sin demora, los derechos de acceso de aquellos de sus usuarios que ya no necesiten acceder a la información y/o los sistemas de información de Airbus por motivos profesionales o contractuales.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.36 - 1	El Proveedor enviará una notificación inmediatamente a Airbus en relación con cualquier revocación de derechos de acceso de usuarios cuando exista una necesidad de acciones administrativas por parte de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.37 - 3	El Proveedor certificará al menos una vez al año que sus usuarios de los sistemas de IT, OT o IoT de Airbus son legítimos y están autorizados de acuerdo con lo estipulado por contrato. *Nota : El Proveedor revelará la lista de los usuarios del sistema al titular del negocio de Airbus del contrato o paquete de trabajo.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.5

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.38 - 3	El Proveedor garantizará que se registren los accesos al sistema o a la red, y que los registros se conserven durante al menos doce meses. *Nota 1 : El Proveedor tomará las medidas adecuadas para garantizar que las transacciones no puedan ser rechazadas.* *Nota 2 : En aquellos países en los que la conservación del registro esté restringida por las leyes y normativas a menos de 12 meses, el Proveedor conservará los datos del registro en la medida en que las leyes y normativas lo permitan.* *Nota 3 : El registro incluye también la creación/modificación/revocación de los derechos de acceso y las credenciales del usuario.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.4.1
ABR.SEC.A1015.0.39 - 1	El Proveedor se asegurará de que los usuarios con derechos de acceso elevados (por ejemplo, administradores) sean supervisados para identificar actividades anormales, aparte del registro de sus accesos al sistema y a la red y sus privilegios de uso.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.4.1 ; ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.40 - 2	El Proveedor garantizará que los sistemas en los que se almacenan o procesan los datos de Airbus o desde los que se acceden a los datos de Airbus estén protegidos contra accesos no autorizados. *Nota : Se requieren mecanismos de seguridad adecuados en todas las capas, como la red (lo cual incluye, entre otros, cortafuegos aplicados y configurados adecuadamente en el perímetro, acceso restringido a internet y la red inalámbrica, conexiones entre cliente y proveedor, acceso remoto VPN), sistemas operativos y aplicaciones (incluida la autentificación y la gestión de usuarios).*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.1.2 ; ISO 27001-2013-A.9.4.1 ; ISO 27001-2013-A.13.1.3

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.41 - 2	El Proveedor se asegurará de que todos los usuarios de la red y los dispositivos informáticos dispongan de identificadores de usuario únicos. *Nota 1 : Esto incluye también las cuentas de administrador. No se utilizará ningún identificador compartido o de grupo, garantizando así la confidencialidad de los sistemas y de la información y la rendición de cuentas en relación con la actividad de los usuarios de la red.* *Nota 2 : Las cuentas de servicio utilizadas por los procesos del sistema y para las comunicaciones máquina a máquina deben tener un propietario claro y gestionarse de forma segura, por ejemplo, restringiendo el acceso interactivo, con una contraseña de complejidad elevada y normas de expiración.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.1
ABR.SEC.A1015.0.42 - 2	El Proveedor se asegurará de que los administradores tengan cuentas separadas para actividades que requieran un nivel elevado de privilegios y para actividades de uso normal (IT, OT o IoT) de trabajo (incluido el uso de internet y del correo electrónico) que no exija ese nivel elevado de privilegios con el fin de evitar que, con el nivel superior de privilegios, se pueda descargar y ejecutar algún código malicioso. *Nota : Las cuentas no privilegiadas se configurarán conforme al principio de "privilegios mínimos" como para cualquier otro usuario normal del Proveedor.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.3
ABR.SEC.A1015.0.43 - 2	El Proveedor se asegurará de que todos los accesos a sus sistemas y a la información estén controlados mediante el uso de contraseñas seguras y sus correspondientes identificadores de usuarios (con las últimas tecnologías). *Nota : Se pueden sustituir por certificados digitales personalizados que cumplan los criterios internacionales acordados.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.2.1

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.44 - 2	El Proveedor aislará la Información de Airbus de su propia información y de la de otros clientes, de modo que solo el personal autorizado pueda acceder a la Información de Airbus. *Nota : El Proveedor no utilizará las mismas zonas de trabajo físicas ni los mismos sistemas de IT, OT o IoT o instalaciones de aplicaciones para Airbus y para los competidores de Airbus sin consultar al Departamento de Seguridad de Airbus.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.45 - 1	El Proveedor no proporcionará acceso a la Información o sistemas de Airbus a ninguna otra entidad sin la aprobación previa y por escrito de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.8 Requisitos : Criptografía

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.46 - 2	El Proveedor utilizará herramientas criptográficas (p. ej. encriptado, firma digital) compatibles con los criterios aplicados por Airbus (interoperabilidad) con el fin de garantizar la confidencialidad y la integridad y no rechazo de los datos que se transfieren y/o almacenan a petición de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.10.1.1
ABR.SEC.A1015.0.47 - 1	Para proyectos o programas clasificados por defensa, el gobierno, la OTAN o la OCCAR, el Proveedor empleará las mismas herramientas criptográficas que Airbus por motivos de cumplimiento e interoperabilidad. *Nota : Airbus puede tener la obligación de utilizar herramientas criptográficas específicas en el contexto de determinados programas o proyectos si así lo solicitan las autoridades o el cliente.*	Proveedor : proveedor de cualquier tipo de bienes o servicios a Airbus clasificados por defensa, el gobierno, la OTAN o la OCCAR.	Documento interno de Airbus
ABR.SEC.A1015.0.48 - 2	Cuando la legislación aplicable restrinja el uso del encriptado, el Proveedor evaluará y acordará con Airbus mecanismos de protección de la información alternativos y adecuados, que se estudiarán caso por caso.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.18.1.5

2.9 Requisitos : Seguridad Física y Medioambiental

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.49 - 2	El Proveedor se asegurará de que el acceso a sus edificios, oficinas e instalaciones informáticas será controlado y limitado (por ejemplo, mediante el uso de puertas con cerradura, lectores de tarjetas, sistemas de prevención de robos, detección y respuesta, etc...) con el fin de proteger de manera eficiente la confidencialidad de la información y el acceso a sistemas clave y activos, y de evitar el robo de documentos o equipos.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.11.1.1
ABR.SEC.A1015.0.50 - 2	El Proveedor limitará adicionalmente el acceso a ciertas zonas concretas : – zonas que alberguen infraestructura de IT, OT o IoT, como salas de servidores o redes, – zonas en las que trabajen usuarios con un alto nivel de privilegios de acceso, – zonas con un nivel alto de confidencialidad para Airbus (conforme a un acuerdo específico).	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.11.1.1
ABR.SEC.A1015.0.51 - 2	El Proveedor se asegurará de que los equipos de IT, OT o IoT clave para el negocio se instalen en una ubicación en la que se reduzcan los riesgos medioambientales (por ejemplo, terremotos, inundaciones o condiciones meteorológicas extremas), y se apliquen controles medioambientales adecuados para mitigar cualquier posible daño físico (por ejemplo, racks/cajas, conductos para cables, sistema de refrigeración, Sistema de alimentación ininterrumpida (UPS), detección de agua, detección/extinción del fuego, gestión de materiales peligrosos, etc...).	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.11.1.4 ; ISO 27001-2013-A.11.2.1
ABR.SEC.A1015.0.100 - 1	El Proveedor deberá implementar una política de escritorio despejado de papeles y medios de almacenamiento extraíbles y una política de pantalla limpia de recursos de procesamiento de información relacionada con el trabajo de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.10 Requisitos : Operaciones de Seguridad

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.52 - 2	El Proveedor se asegurará de que se establezcan en su seno unos procedimientos de control de cambios formales para garantizar que todas las modificaciones realizadas en los sistemas e infraestructura de IT, OT o IoT (por ejemplo, configuraciones, actualizaciones, nuevas aplicaciones o componentes, etc...) queden debidamente documentadas, probadas y aprobadas por el departamento de IT, OT o IoT del Proveedor y/o por gestión empresarial.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.1.2 ; ISO 27001-2013-A.12.1.4
ABR.SEC.A1015.0.53 - 1	Salvo en la medida en que se disponga lo contrario en el contrato entre Airbus y el Proveedor, el Proveedor obtendrá el consentimiento específico del departamento de Seguridad de Airbus antes de procesar cualquier cambio que involucre a los sistemas o datos de Airbus o que pueda afectar a los ámbitos de confidencialidad, disponibilidad, integridad y rendición de cuentas.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.54 - 1	El Proveedor realizará copias de seguridad de datos y software con regularidad y respetará los siguientes principios : – almacenar las copias de seguridad fuera de los sistemas activos, – proteger físicamente el almacenamiento de copias de seguridad al menos con el mismo nivel que los sistemas activos, – realizar pruebas periódicas de restauración de copias de seguridad.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.3.1
ABR.SEC.A1015.0.55 - 2	El Proveedor se asegurará de que el equipo clave de IT, OT o IoT esté cubierto por una garantía del fabricante o por el soporte de la organización, garantizando así la disponibilidad de los sistemas y la información.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.11.2.4
ABR.SEC.A1015.0.56 - 2	El Proveedor prestará todo el cuidado y utilizará todos los medios disponibles, incluida la tecnología más avanzada que sea necesaria para impedir la intrusión de códigos maliciosos en todo su equipo de IT, OT o IoT, en los medios de almacenamiento y en toda la infraestructura posible (por ejemplo, servidores, pasarelas de correo, etc...) con el fin de evitar la corrupción de los datos o la pérdida del servicio.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.2.1

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.57 - 1	El Proveedor se asegurará de que los patrones/firmas de los mecanismos contra la intrusión y/o antivirus se actualicen con regularidad en todos los dispositivos, incluidos los móviles.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.2.1
ABR.SEC.A1015.0.58 - 1	El Proveedor se asegurará de que se apliquen los parches críticos a todos los sistemas, de acuerdo con las recomendaciones de los distribuidores de software, una vez que el Proveedor haya probado su compatibilidad con sus instalaciones.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.12.6.1
ABR.SEC.A1015.0.59 - 1	El Proveedor aplicará mecanismos adecuados de Prevención de pérdida de datos con el fin de evitar la divulgación no autorizada de la Información de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.11 Requisitos : Seguridad de las Comunicaciones

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.60 - 1	El Proveedor cumplirá los criterios y procedimientos de intercambio de datos y conectividad de Airbus, salvo que Airbus acuerde lo contrario por escrito.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.13.2.1
ABR.SEC.A1015.0.61 - 1	En caso de que los datos de Airbus tengan que ser transferidos a través de redes de datos que no estén bajo el control directo del Proveedor (por ejemplo, líneas alquiladas, internet), el Proveedor realizará todas las acciones que correspondan para garantizar tanto la confidencialidad como la integridad de los datos en tránsito.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.13.2.2 ; ISO 27001-2013-A.13.1.1

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.62 - 2	El Proveedor se asegurará de que el tráfico de datos desde y hacia internet u otras redes que no sean de confianza (p. ej. entornos de pruebas, redes de socios) se limite mediante mecanismos de seguridad sólidos y se supervise para identificar conductas anormales, por ejemplo, utilizando *proxies* y pasarelas. *Nota 1 : Las direcciones de internet que se sepa que representan un riesgo de uso incorrecto o una fuente de ataques serán bloqueadas. Esto mismo se aplica en el caso de correos electrónicos potencialmente peligrosos, como spam, phishing y archivos adjuntos sospechosos.* *Nota 2 : El Proveedor impedirá también que los usuarios eludan esos mecanismos de control (por ejemplo, usuarios que recurran a la tunelización a proxies alternativos, que utilicen correos web o servicios personales en la nube para compartir datos empresariales o para descargar material no autorizado).*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.13.2.3
ABR.SEC.A1015.0.63 - 2	El Proveedor utilizará únicamente equipos que hayan sido aprobados por Airbus para conectarse a las redes, sistemas o productos de Airbus (a excepción de los "Portales de proveedores"). *Nota : El equipo de la red de Airbus deberá poder ser supervisado y parcheado (incluyendo actualizaciones antimalware) por Airbus. El equipo propio del Proveedor que no cumpla este requisito solo podrá conectarse a redes aisladas de Airbus.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.13.1.3

2.12 Requisitos : Adquisición de Sistemas, Desarrollo y Mantenimiento

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.64 - 2	El Proveedor se asegurará de que los productos entregados a Airbus que contengan componentes de IT, OT o IoT (lo cual incluye, entre otros, aplicaciones de software, equipo de fabricación con instalaciones informáticas integradas o sistemas de control industrial y gestión de edificios) se desarrollen utilizando una metodología de desarrollo de sistemas estructurada y aprobada que garantice que los requisitos de seguridad de la información se tienen en cuenta como parte del proceso y se definen, documentan y cumplen en consecuencia mediante el uso de normas de codificación seguras y verificadas en la fase de prueba y aceptación.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.14.2.1
ABR.SEC.A1015.0.65 - 2	Si es necesaria su instalación o conexión en el entorno de IT, OT o IoT de Airbus, el Proveedor se asegurará de que los productos que entregue a Airbus puedan integrarse en los procesos de seguridad de la red de Airbus, como protección contra software malintencionado, parcheado, control de acceso, supervisión de incidentes y registro. *Nota : Los productos entregados a Airbus por el Proveedor que contengan componentes de IT, OT o IoT, incluyendo, entre otros, aplicaciones de software, equipos de fabricación con instalaciones informáticas integradas y sistemas de control industrial y gestión de edificios.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.66 - 2	El Proveedor se asegurará de que su mantenimiento y soporte remoto para productos entregados a Airbus cumpla los criterios de conexión remota de Airbus. *Nota : Los productos entregados a Airbus por el Proveedor que contengan componentes de IT, OT o IoT, incluyendo, entre otros, aplicaciones de software, equipos de fabricación con instalaciones informáticas integradas y sistemas de control industrial y gestión de edificios.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.9.1.2

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.99 - 1	Cuando el Proveedor tenga que conectar su propio equipo de IT, OT o IoT a alguno de sus propios productos en fabricación en Airbus o incorporados a un producto de Airbus (avión, helicópteros, satélites, drones, etc...) para configurarlos, cargar datos o software, o probar o resolver problemas en un entorno de fabricación, entrega o mantenimiento de Airbus, el Proveedor se asegurará de que dicho equipo de IT, OT o IoT y el software que incluye : – sean específicos y restringidos para ese tipo de actividad y su uso esté sujeto a procedimientos formales, – no estén conectados a ninguna otra red que la interna del producto durante la operación en el producto de Airbus. – estén autenticados, intactos, no tengan defectos y no contengan software malintencionado, lo que incluye también todos los medios extraíbles conectados a dicho equipo.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.13 Requisitos : Relaciones con los Proveedores

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.67 - 2	En caso de que sea necesario que el Proveedor conceda acceso a la Información de Airbus a alguno de sus proveedores y/o subcontratistas, el Proveedor notificará a Airbus y transferirá todos los requisitos de este documento al proveedor y/o subcontratista del nivel inferior a través de un acuerdo específico. *Nota 1 : El Proveedor será el único responsable de la aplicación de los requisitos de seguridad de Airbus en su propia cadena de suministro.* *Nota 2 : Además de sus actividades industriales, este requisito también abarca la subcontratación de IT, OT o IoT y proveedores en la nube, así como la gestión de instalaciones y servicios afines con acceso a Información de Airbus.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.68 - 2	Cuando Airbus lo solicite, el Proveedor le entregará el acuerdo en relación con los requisitos de seguridad entre el Proveedor y un proveedor y/o subcontratista de nivel inferior. *Nota : Este acuerdo no establecerá en ningún caso una relación contractual directa entre Airbus y los proveedores y/o subcontratistas del Proveedor.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.1.1
ABR.SEC.A1015.0.69 - 2	El Proveedor realizará revisiones de seguridad y riesgos con el fin de verificar el cumplimiento de esta Directiva por parte de su subcontratista. *Nota 1 : El Proveedor también será responsable de comunicar los incumplimientos detectados al departamento de seguridad de Airbus.* *Nota 2 : Airbus se reserva el derecho a evaluar adicionalmente a los proveedores y/o subcontratistas del Proveedor en relación con esta Directiva ; esta evaluación podrá ser realizada por el departamento de Seguridad de Airbus o un auditor independiente que se haya acordado.* *Nota 3 : El Proveedor está autorizado a nombrar a un auditor independiente acordado para esta tarea.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.2.1

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.70 - 2	El Proveedor no concederá acceso bajo ningún concepto a los datos o sistemas de Airbus (incluyendo, entre otros, mediante enrutamiento o sistema en serie) a ninguno de sus proveedores y/o subcontratistas sin la autorización previa y por escrito de Airbus.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.14 Requisitos : Gestión de Incidentes de Seguridad de la Información

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.71 - 1	El Proveedor realizará una supervisión continua de los sistemas y las redes, empleará sistemas de detección y prevención de intrusiones y registrará los eventos de seguridad.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.72 - 1	El Proveedor contará con controles adecuados para identificar y hacer frente a ciberataques sofisticados, como Amenazas persistentes avanzadas (APT, por sus siglas en inglés) y canales de Mando y control.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.73 - 2	El Proveedor aplicará un proceso exhaustivo y aprobado en la gestión de incidentes relacionados con la información y sistemas que incluya identificación, respuesta, recuperación, elaboración de informes, protección de pruebas y revisión posterior a la aplicación de los incidentes de seguridad de la información. *Nota : Los incidentes incluyen, entre otros : pérdida o robo de equipos, averías, pérdidas de potencia, sobrecargas, errores de usuarios/personal de IT, OT o IoT, violaciones de acceso, software malintencionado y pirateo.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.16.1.1
ABR.SEC.A1015.0.74 - 2	El Proveedor identificará y resolverá los puntos débiles e incidentes de seguridad, minimizará su impacto empresarial y reducirá el riesgo de que se produzcan incidentes similares.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.16.1.1

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.75 - 2	En caso de que los incidentes de seguridad se produzcan de tal manera que puedan afectar a los sistemas o a la Información de Airbus, el Proveedor investigará e informará del incidente sin demora al departamento de seguridad de Airbus, incluso aunque no se le solicite. *Nota : Estos incidentes incluyen, entre otros, el robo de equipos que tienen almacenada información de Airbus, filtración de datos de Airbus de los sistemas del Proveedor y puesta en riesgo de los sistemas conectados a Airbus.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.2.1 ; ISO 27001-2013-A.16.1.2
ABR.SEC.A1015.0.76 - 2	El Proveedor realizará cualquier acción para rectificar incidentes de seguridad detectados o que se le hayan comunicado. *Nota : En caso de que Airbus detecte en sus propios sistemas algún tipo de incidente de seguridad originado por el Proveedor, Airbus lo notificará inmediatamente a este y se reserva el derecho a interrumpir temporalmente o restringir la conectividad con el Proveedor.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.16.1.5

2.15 Requisitos : Aspectos Relacionados con la Seguridad de la Información en la Gestión de la Continuidad del Negocio

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.77 - 2	El Proveedor tendrá preparado un Programa de continuidad del negocio para mantener o restaurar los servicios de IT, OT o IoT en caso de fallo grave o cualquier tipo de acontecimiento de fuerza mayor (incluyendo, entre otros : daño físico, cortes de energía, incendios o catástrofes naturales). *Nota : Este programa consiste en el Marco de gestión, los Planes de continuidad del negocio, Mantenimiento, Revisión y pruebas y Reanudación del negocio y recuperación ante desastres.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.17.1.1

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.78 - 1	Marco de gestión : el Proveedor contará con mecanismos, procesos, funciones definidas y responsabilidades adecuados para garantizar la continuidad de los procesos de negocio y evitar interrupciones graves. *Nota : Esto debería abarcar la Identificación y evaluación de riesgos, las estrategias de mitigación y el mantenimiento de la disponibilidad de los servicios, procesos y productos del negocio mediante concienciación, revisiones y pruebas.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.17.1.1
ABR.SEC.A1015.0.79 - 1	Planes de continuidad del negocio : el Proveedor documentará y formará a sus empleados en relación con sus planes de continuidad del negocio con el fin de garantizar que el negocio siga funcionando a un nivel efectivo en caso de incidente grave.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.17.1.2
ABR.SEC.A1015.0.80 - 1	Mantenimiento, revisión y pruebas : el Proveedor tendrá que poder demostrar que se realiza una revisión, mantenimiento y pruebas periódicas de los planes mediante ejercicios.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.17.1.3
ABR.SEC.A1015.0.81 - 2	Reanudación del negocio y recuperación ante desastres : el Proveedor elaborará un Plan de recuperación ante desastres para su actividad relacionada con Airbus y los sistemas y procesos internos dependientes de este. *Nota : Esto incluye la planificación y los pasos detallados a realizar durante y después de un incidente para que las operaciones del negocio puedan retomarse y volver a su estado normal.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.17.1.2

2.16 Requisitos : Cumplimiento

Tanto Airbus como el Proveedor se comprometen a cumplir todos los requisitos jurídicos (en concreto, cuando el acuerdo de acceso sea internacional y abarque distintas jurisdicciones). Estos requisitos pueden variar en función del Proveedor y estarán sujetos a revisión caso por caso.

Se prestará especial atención a los conflictos de leyes relacionados principalmente con la protección de datos/privacidad, supervisión, conservación de datos y criptografía.

El Proveedor reconoce que Seguridad de Airbus o un auditor independiente nombrado por Airbus podrá auditar la seguridad de los sistemas, procesos y procedimientos del Proveedor que puedan incluir sistemas o Información de Airbus o desde los que se pueda acceder a ellos.

Airbus se reserva el derecho, previa notificación con una antelación razonable, a realizar auditorías de cumplimiento y/o implantación a su discreción.

Airbus se reserva el derecho a interrumpir o restringir la conectividad o el acceso a información por parte del Proveedor en caso de que se deniegue el acceso al auditor, no se implementen las acciones correctoras o no haya colaboración en caso de un incidente de seguridad grave.

En caso de cambio significativo en la situación del Proveedor (incluyendo, entre otras cosas, fusiones, adquisiciones u otras reorganizaciones corporativas) o en sus actividades empresariales, Airbus se reserva el derecho a reevaluar el cumplimiento por parte del Proveedor de los requisitos de seguridad de Airbus necesarios para proteger los activos de información e infraestructura asociados a Airbus.

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.82 - 1	El Proveedor garantizará una revisión regular y una auditoría de : – la fortaleza técnica de sus sistemas, – su cumplimiento de la política, – sus procedimientos de protección de sistemas e información.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.18.2.1
ABR.SEC.A1015.0.83 - 1	El Proveedor cumplirá todas las leyes aplicables en materia de propiedad intelectual/derechos de autor y obtendrá todas las licencias de software necesarias.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.18.1.2
ABR.SEC.A1015.0.84 - 2	El Proveedor proporcionará a Airbus (o a un auditor independiente que se haya acordado) acceso a los edificios, documentos, sistemas, etc... a efectos de inspeccionar y validar las medidas de seguridad con arreglo a esta Directiva y para la mitigación de riesgos relacionados con la seguridad de la información. *Nota : Este acceso también puede incluir la cadena de suministro del Proveedor cuando se considere que se realiza intercambio de datos o conectividad a los sistemas de Airbus.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.2.1

Referencia	***Denominación***	***Condición de aplicabilidad***	***Origen***
ABR.SEC.A1015.0.85 - 1	El Proveedor tomará todas las medidas necesarias para proporcionar información adecuada a Airbus para la realización de la evaluación de seguridad, ya sea por Airbus o por un auditor independiente.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.15.2.1
ABR.SEC.A1015.0.86 - 1	El Proveedor tomará todas las medidas correctoras necesarias en relación con cualquier defecto detectado por el auditor.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.88 - 2	El Proveedor podrá aportar pruebas a Airbus que demuestren que su organización cumple las leyes y normativas de exportaciones y que mantiene la debida trazabilidad, de modo que pueda cumplir cualquier control. *Nota : Airbus podrá comprobar en cualquier momento la fiabilidad de la organización del Proveedor en relación con esos requisitos (físicos y lógicos), lo que incluye, entre otros, que se garantice la identidad y nacionalidad (o nacionalidades) de los usuarios, la aprobación y el control del acceso a la información (incluyendo un proceso formal de acreditación de usuarios), el control del flujo de información y los registros de auditoría.*	Proveedor : proveedor de cualquier tipo de bienes, datos técnicos o servicios a Airbus sometido a las leyes y normativas de control de exportaciones.	Documento interno de Airbus
ABR.SEC.A1015.0.90 - 2	En caso de que la relación contractual exija que el Proveedor acceda a información clasificada por defensa, el gobierno, la OTAN o la OCCAR, el Proveedor aplicará medios técnicos y organizativos para cumplir la Ley de secretos de estado del país en el que ejecute el contrato, de acuerdo con los niveles de clasificación indicados por Airbus en las Instrucciones de seguridad del programa específico o en la Carta sobre aspectos relativos a seguridad.	Proveedor : proveedor de cualquier tipo de bienes, datos técnicos o servicios a Airbus clasificados por defensa, el gobierno, la OTAN o la OCCAR.	Documento interno de Airbus
ABR.SEC.A1015.0.91 - 1	El Proveedor proporcionará información y colaborará con Airbus para responder a cualquier requerimiento, investigación o situación similar con el fin de conseguir Información de Airbus y proporcionará información y asistencia a Airbus para obtener una certificación en relación con su Información, incluida aquella Información en posesión del Proveedor.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.92 - 2	El Proveedor notificará rápidamente a Airbus tras la recepción de una solicitud que exija la entrega de Información de Airbus a cualquier tercero, incluidas las administraciones o autoridades públicas. *Nota : El Proveedor utilizará todos los medios legales para oponerse a dichas solicitudes de acceso, salvo que Airbus lo haya aprobado.*	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus

2.17 Requisitos : Rescisión/Separación

Referencia	*Denominación*	*Condición de aplicabilidad*	*Origen*
ABR.SEC.A1015.0.93 - 1	En el momento de la firma del Contrato, o con anterioridad, el Proveedor facilitará a Airbus un plan de rescisión que contemple el modo en que se devolverá a Airbus la Información de Airbus al final de este contrato, incluidas las copias de seguridad y la información en archivos, y el modo en que se eliminará la Información de Airbus del equipo e instalaciones del Proveedor de manera permanente.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.94 - 1	El Proveedor garantizará la protección de la Información y los sistemas de Airbus, incluyendo la continuación del servicio al expirar el Contrato/acuerdos contractuales en cumplimiento de lo dispuesto en los mismos.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	Documento interno de Airbus
ABR.SEC.A1015.0.95 - 1	El Proveedor informará de inmediato a Airbus en caso de que deje de ser necesario acceder a todos o a alguno de los datos o sistemas de Airbus para cumplir sus obligaciones en virtud del Contrato/acuerdos contractuales.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.1.4
ABR.SEC.A1015.0.96 - 1	Tras la expiración del plazo acordado para el uso de la información o cuando la información deje de ser necesaria, el Proveedor eliminará la información conforme a lo acordado con Airbus para garantizar que no se pueda recuperar.	Proveedor : proveedor de cualquier tipo de bien o servicio a Airbus.	ISO 27001-2013-A.8.1.4

3 Documentos de Referencia

Los documentos indicados a continuación se han utilizado para crear esta Directiva. Sin embargo, no se consideran parte integrante del Contrato/acuerdo contractual entre Airbus y el Proveedor basado en esta Directiva, salvo que se indique y se haga referencia a ellos en los requisitos correspondientes. Airbus proporcionará al Proveedor los documentos de referencia bajo petición.

Nótese bien : Cualquier documento de ISO o ISF será facilitado directamente por el Proveedor, Airbus no puede entregar esos documentos por motivos de derechos de autor.

Referencia doc.	***Título***
A1044	Requisitos de Seguridad para la Clasificación y Protección de la Información (*Security Requirements for Classification and Protection of Information)*
GTC	Términos y Condiciones Generales de Acceso y Uso de los Portales de Proveedores de Airbus *(General Terms and Conditions for Access to and Use of Airbus Supplier Portals)*
ICT/IST Charter	Gestión de la Información de Airbus - Uso de las instalaciones de IST *(Airbus Information Managements - Use of IST Facilities)*
ISO/IEC 27001	Tecnología de la información - Sistemas de gestión de la seguridad de la información - Requisitos *(Information technology - Information security management systems - Requirements)*
ISO/IEC 27002	Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información *(Information technology - Security techniques - Code of practice for information security controls)*
ISO/IEC 27003	Tecnología de la información - Técnicas de seguridad - Seguridad de la información *(Information technology - Security techniques - Information security)*
ISO/IEC 27036	Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con los proveedores - Guía para la implementación del sistema de gestión *(Information technology - Security techniques - Information security for supplier relationships management system implementation guidance)*
IEC 62443 Part 2-1 2010	Redes de comunicación industrial - Seguridad de la red y sistemas - Establecer un programa de seguridad para el sistema de control y automatización *(Industrial communication networks - Network and system security -Establishing an industrial automation and control system security program)*
SoGP April 2016	Norma ISF de buenas prácticas para la seguridad de la información *(The ISF Standard of Good Practice for Information Security)*

4 Glosario

Referirse siempre a LEXINET

Airbus	Se refiere a Airbus S.A.S. y sus filiales, sucursales, empresas conjuntas y empresas asociadas
Cíber	En el contexto de esta Directiva, se refiere al mundo dinámico, siempre en línea y tecnológicamente interconectado ; está formado por personas, organizaciones, información y tecnología. Cambia constantemente en maneras impredecibles y facilita la colaboración, pero plantea el riesgo de actividades criminales, concentra los objetivos y oculta a los infractores
Continuidad del negocio	En el contexto de esta Directiva, se refiere a la capacidad estratégica y táctica de la organización del Proveedor para planificar y responder a incidentes e interrupciones de la actividad con el fin de proseguir las operaciones del negocio a un nivel aceptable para garantizar el cumplimiento del contrato
Datos	En el contexto de esta Directiva, se refiere a toda la información electrónica en cualquier formato y medio
Departamento de Seguridad de Airbus	En el contexto de esta Directiva, se refiere a la organización y personas de Airbus responsables de proteger al personal, la información, las actividades, el patrimonio científico y tecnológico, los activos y la reputación de Airbus frente cualquier acción hostil como método de prevención, detección y respuesta a esas acciones hostiles
Gestión de riesgos	Un proceso de gestión prospectivo que anticipa los posibles Riesgos para los objetivos de negocio del Proveedor y se encarga de su mitigación con el fin de que los Sistemas de información no se vean expuestos (o, por su parte, afecten a los procesos de negocio de los que se encarga) a consecuencias que se podrían haber previsto y evitado razonablemente
Información de Airbus	En el contexto de esa Directiva, se refiere a los derechos de propiedad intelectual, métodos, conocimientos técnicos, tecnología y procesos registrados y/o privilegiados y hechos y cifras internas de Airbus, así como cualquier material o documento relacionado. Se incluyen todos los medios y métodos de almacenamiento y transmisión posibles, en cualquier formato y en cualquier formato (incluyendo, entre otros, documentos en papel, impresiones, microfichas, datos electrónicos en cualquier formato, imágenes y archivos multimedia)
Internet de las cosas o IoT	En el contexto de esta Directiva, es la red de dispositivos físicos, vehículos u otros elementos que tienen incorporado software, sensores, actuadores y conectividad a la red que permiten a esos objetos recoger e intercambiar datos. Cada cosa se identifica exclusivamente a través del sistema informático que tiene incorporado, pero puede interactuar dentro de la infraestructura de internet existente
ISF	Foro de Seguridad de la Información *(Information Security Forum)*
ISMS	Sistema de Gestión de la Seguridad de la Información *(Information Security Management System)*
OCCAR	Organización Conjunta de Cooperación en Materia de Armamento *(Organisation Conjointe de Coopération en matière d'Armement)*
OTAN	Organización del Tratado del Atlántico Norte

Proveedor	En el contexto de esta Directiva, se refiere a aquellas entidades que proporcionan bienes y/o servicios en beneficio de Airbus y que no forman parte de Airbus (lo cual incluye, entre otros, proveedores, subcontratistas, socios industriales y centros de investigación)
Riesgo	En el contexto de esta Directiva, se refiere a un acontecimiento o condición que, si se produce, tendría un impacto negativo sobre los objetivos y el cumplimiento del contrato por parte del Proveedor en términos de diseño, producción y/o entrega futura de productos o servicios a Airbus
Seguridad de la información	Medios de proteger : – la disponibilidad : impedir la pérdida de información y servicios, como, por ejemplo, debido a código malintencionado, desastres naturales, fallos o anomalías del sistema, etc..., – la integridad : para impedir la entrada de información no autorizada, la modificación, el procesamiento y la eliminación de datos, – la confidencialidad : para evitar la divulgación no autorizada, – la responsabilidad : para garantizar que se conoce la identidad de los usuarios, que se puede exigir responsabilidades individuales y se pueden rastrear accesos y transacciones con fines de auditoría para impedir y detectar intrusiones fraudulentas
Tecnología de la información o IT	En el contexto de esta Directiva, se refiere a cualquier tecnología de la información o equipo o servicio de telecomunicaciones, software y procesos asociados para el almacenamiento, procesamiento y transmisión de datos. En concreto, incluye PC, estaciones de trabajo, portátiles, medios extraíbles, teléfonos, smartphones, redes, sistemas, programas informáticos, servidores, bases de datos y portales web
Tecnología operativa u OT	En el contexto de esta Directiva, se refiere a cualquier tecnología de gestión de datos o comunicación, o equipos o servicios de telecomunicaciones, firmware, software y procesos asociados para el almacenamiento, procesamiento y transmisión de datos incorporados en el equipo de fabricación (OT). Incluye principalmente : interfaz hombre-máquina, interfaz de primera línea, medios extraíbles, redes, controladores lógicos programables (PLC) utilizados en los controles de fabricación y construcción

Colaboradores

Nombre	***Función***
ALTSTÄDT Kai	Prod. Indust & Operational Security MGR - EIDS
BALLARD Florence	Security Business Partners - ZSB
BOUDET Florent	Security Assurance - ZSG
DENIS Pierrette	Security Operations - ZSO
GAUVRY Philippe	Q Procurement Requirements Proj Mgr - QPR
JORDAN Marie	Prod. Secur capabilities Compliance MGR - EIDC1
MEIER-HEDDE Felix	Prod. Indust & Operational Security MGR - EIDS
REY Nathalie	Prod. Indust & Operational Security MGR - EIDS
THORNARY Mathieu	IM Security Analyst - ZIST
TREDEZ Juliette	Governance - ZSG
UTH Fridtjof	Security Assurance - ZSG

Traducción Aceptable para Despliegue en la Lengua Local

Función	***Nombre***	***Fecha***
Traducción en Español Aprobada	**GIL Miguel Angel**	**30/05/18**

Registro de las Revisiones

Edición	***Fecha***	***Resumen y razones para cambios***
A	Dic 2017	Índice inicial. Documento revisado íntegramente. Fusión de A1015 de Airbus y el anterior E260 de Airbus Group, con inclusión de los requisitos de Airbus Helicopters y Airbus Defence&Space, y aspectos de producto/OT.
	Jun 2018	**La versión traducida en español está a disposición.**