

Annex B Information System Security

Introduction

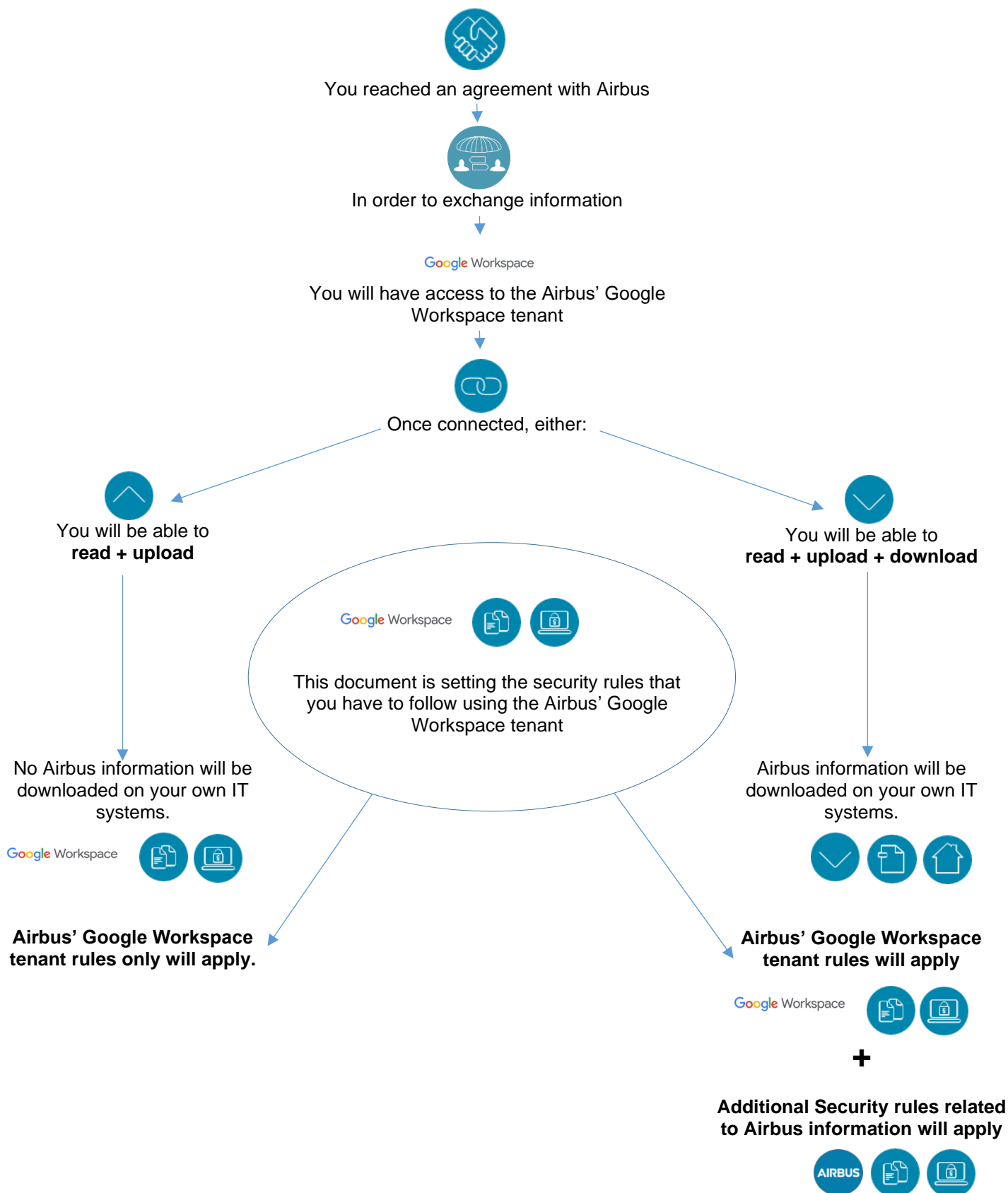


Table of contents

Agreement on Collaborative Working	2
Security Policies	2
Organization of Security	3
Human Resources Security	3
Asset management	4
Access Control	4
Cryptography	6
Physical and Environmental Security	6
Operations Security	7
Communication Security	7
Supplier Relationships	8
Information Security Incident Management	8
Compliance	9
Termination / Disengagement	11

Main Terms and Conditions

Agreement on Collaborative Working

Related to Google Workspace Services

The Company shall implement a baseline protection in accordance with the STC, prior to or upon usage of Airbus Google Workspace Services.

The Company shall only access, use, modify, and/or remove any aspects of Airbus system(s) in relation with the Google Workspace Services or Airbus data as authorized by Airbus.

Note: the Company does not attempt to access any systems or information that has not been authorized by Airbus for contract execution.

The Company shall protect from loss, destruction, falsification, corruption, unauthorized access and unauthorized release, all relevant Airbus Content that it accesses, operates or processes using Google Workspace Services.

Security Policies

Related to Google Workspace Services

The Company 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 Company's information and systems.

Based on its information security policy, the Company shall establish a comprehensive set of information security documentation (a combination of policies, standards and procedures) aimed at privileged users (e.g. administrators, programmers) to ensure consistent implementation of information security controls.

Organization of Security

Related to Google Workspace Services

Related to the Company's own environment

Appointment of Security Manager – the Company shall nominate one of its employees with overall accountability for security and risk issues and provide appropriate authority and means to this function to coordinate the activity across the organization.

This Company's Security Manager shall be aware of all applicable statutory and contractual requirements, including but not limited to those laid down in this Annex and export compliance, affecting the Company's security controls, processes and systems.

The Company 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.

Human Resources Security

Related to Google Workspace Services

Related to the Company's own environment

Solely the Company shall be responsible for the enforcement of Airbus security requirements within its organization and therefore ensures that the users are qualified and properly trained, as defined in the STC.

The Company shall have in place systematic staff vetting processes for checking identity and background of its personnel.

The Company shall ensure that all employees and suppliers/subcontractors who have access to Airbus Content are made aware of the confidential nature of that information and of the obligations contained in the STC, through appropriate training and awareness activities.

The Company shall ensure that contracts with its employees and suppliers/ subcontractors, under the scope of the activities conducted through Google Workspace Services, comply with the confidentiality commitments contained in this STC.

With respect to systems related to Google Workspace Services, the Company 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 Company undertakes that any replacement staff has an equivalent level of competence.

Asset management

Related to Google Workspace Services

Related to the Company's own environment

Upon request, the Company shall provide Airbus with a list of all the systems and devices where Airbus Content is stored or processed (i.e. physical location, network location and business purpose of storing/processing).

The Company shall not store Airbus Content on mobile devices (Smartphone's, laptops, USB drives, etc.) unless encrypted by state of the art products/standards.

Any used or broken storage media containing Airbus Content shall be effectively wiped or destroyed prior to being decommissioned or reused.

Access Control

Related to Google Workspace Services

Related to the Company's own environment

When accessing the Google Workspace Services, the Company shall only use permitted access methods and controls as provided or required by Airbus.

The Company shall maintain an up to date list of user authorizations on systems of its organization relative to the scope of the activities conducted in relation with Google Workspace Services.

The Company shall ensure the user request and authorization process for access rights to the systems relevant to this document is traceable in its organization and complies with the need-to-know principle.

The Company shall revoke, without undue delay, access rights of any Company's user who no longer requires access to Airbus systems and/or information for professional or contractual reasons.

Access control (.../...)

Related to Google Workspace Services

Related to the Company's own environment

The Company shall notify Airbus without undue delay concerning any user access right revocations when there is a need for administrative actions by Airbus.

The Company shall certify at least yearly that its users of Airbus Google Workspace Services are legitimate and authorized as contractually stipulated in the Google Workspace STC.

Note: The Company discloses the list of system users to the Airbus business owner of the contract or work package.

The Company shall ensure that all users of the network and computing devices have a unique personal userID.

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 shall be managed securely e.g. by restricting interactive logon, high password complexity and expiration rules.

For systems relevant to Company's performance under the Google Workspace Services, the Company shall ensure that administrators have separate accounts for high privilege activities and normal usage (IT, OT or IoT) work (incl. Internet and email use) not requiring elevated privileges to prevent malicious code being downloaded and executed under the high privileges.

For systems relevant to Company's performance under the Google Workspace STC, the Company shall use industry standard measures to ensure that all access to its systems and information are controlled by the use of strong passwords and corresponding userIDs.

Access control (.../...)

Related to Google Workspace Services

The Company shall not provide access to Airbus Content or systems to any other entity without prior written approval from Airbus.

Related to the Company's own environment

The Company shall isolate Airbus Content from its own information and other customers' information so that only authorized staff can access Airbus Content.

Cryptography

Related to Google Workspace Services

The Company 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.

Note : The Company needs to ensure that encrypted information remain encrypted all along their life.

Related to the Company's own environment

Physical and Environmental Security

Related to Google Workspace Services

The Company 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.

The Company 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.

Related to the Company's own environment

Operations Security

Related to Google Workspace Services

Related to the Company's own environment

Except as provided for elsewhere under the STC between Airbus and the Company, the Company shall obtain specific agreement from Airbus Security department before processing any change that involves Airbus data where the areas of confidentiality, availability, integrity and accountability may be affected.

The Company shall use all care and means available, including any state of the art or industrial standards 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, email gateways, etc.), in order to prevent data corruption or loss of service.

The Company shall ensure that patterns/ signatures of anti-intrusion and/or anti-virus mechanisms are updated regularly on mobile ones.

The Company shall implement appropriate data loss prevention mechanisms to prevent unauthorized disclosure of Airbus Information.

Communication Security

Related to Google Workspace Services

Related to the Company's own environment

When accessing the Google Workspace Services, the Company shall comply with Airbus data exchange and connectivity standards and procedures, unless agreed otherwise in writing by Airbus.

Should Airbus Content be transferred through data networks which are not under the direct control of the Company (e.g. leased lines, the Internet), the Company shall take all adequate actions to ensure both the confidentiality and the integrity of the data in transit.

The Company 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 (e.g. multiple filtering mechanisms, Denial-of-service protection, exfiltration prevention, IDS/IPS, authenticated proxies for management, gateways).

Note 1: The Company 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).

Note 2: Internet addresses known to be a risk for misuse or source of attacks are blocked. The same applies for potentially dangerous emails like spam, phishing and suspicious attachments.

Supplier Relationships

Related to Google Workspace Services

Related to the Company's own environment

Should there be a need for the Company to give access to Airbus information to one of its suppliers and/or subcontractors for the performance of the activities contemplated by the STC, the Company shall get prior written authorization from Airbus and shall cascade all requirements herein to the lower tier supplier and/or subcontractor by means of a specific agreement.

Under no circumstance shall the Company 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.

The Company shall perform security and risk reviews in connection with the activities contemplated by the Google Workspace STC in order to check the compliance of its subcontractors with this Annex.

Information Security Incident Management

Related to Google Workspace Services

Related to the Company's own environment

For systems under Company's control, the Company shall perform continuous monitoring of systems and networks, employ intrusion detection and prevention systems and record security events.

The Company shall have appropriate controls in place on the systems in which Airbus data will be stored to identify and counter sophisticated cyber-attacks like Advanced Persistent Threats (APT) and Command & Control channels.

The Company 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.

Information Security Incident Management (.../...)

Related to Google Workspace Services

Related to the Company's own environment

The Company shall identify and resolve security weaknesses and incidents, minimize their business impacts and reduce the risk of similar incidents occurrences.

Should security incidents occur that potentially affect Airbus systems or Information, the Company shall investigate and report the incident to Airbus Security without undue delay even without request.

Note: Such incidents include but are not limited to theft of equipment storing Airbus Information, leakage of Airbus data from Company's systems, compromise of systems connected to Airbus.

The Company shall take appropriate action to remedy detected or notified security incidents.

Note 1: Airbus reserves the right to discontinue or restrict Airbus Google Workspace Services for the Company in case corrective actions are not implemented or lack of collaboration in case of a major security incident.

Note 2: Should Airbus detect in its systems any kind of security incident originating from the Company, Airbus notifies the Company immediately and reserves the right to temporarily discontinue or restrict the connectivity with the Company.

Compliance

Both Airbus and the Company undertake to comply with all relevant laws and regulations.

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

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

Related to Google Workspace Services

Related to the Company's own environment

For systems used to perform activities in connection with the Google Workspace STC, the Company shall ensure a regular review and audit of its:

- systems' technical robustness,
- compliance with policy,
- procedures for safeguarding systems and information.

Compliance (.../...)

Related to Google Workspace Services

Related to the Company's own environment

With respect to systems that interface with the Google Workspace Services, the Company shall grant Airbus (or an agreed independent auditor) access to buildings, documents, systems, processes and procedures for the purpose of inspecting compliance with the security measures in line with this Annex and for information security risk mitigation. This access may also flow down into the Company's supply chain, where it is deemed that data exchange or systems connectivity is made to Airbus systems.

Note : Airbus reserves the right to discontinue or restrict Airbus Google Workspace Services for the Company in case audit access is denied.

The Company shall be able to provide any Authority with proof that its organization meets applicable export control laws and regulations and that it keeps the traceability of this so that it can satisfy any control.

The Company shall provide information to and cooperate with Airbus in response to any subpoena, investigation or the like seeking Airbus Content and provide information and assistance to Airbus to seek certification and the like relative to its Content including Content in the possession of the Company.

The Company shall promptly notify Airbus upon the receipt of any request requiring that Airbus Content be supplied to any other third party, including public administrations or authorities.

Note: The Company uses all legal means to contest such access requests unless approved by Airbus.

Termination / Disengagement

Related to Google Workspace Services

Related to the Company's own environment

At or before the time of STC signing, the Company shall provide Airbus with a termination plan that addresses how Airbus Content will be returned to Airbus at the end of the STC, including backup and archival information, and how all Airbus Content will be permanently removed from Company's equipment and facilities.

The Company shall ensure the protection of Airbus Content and systems including continuation of service at the expiry of the Google Workspace Services STC and in compliance with the provisions contained in the Google Workspace Services STC.

The Company shall immediately notify Airbus when access to certain or all Airbus data or systems is no longer needed to fulfill its obligations under the Google Workspace Services STC.