P-15: Supplier Security Policy

1. SUMMARY

1.1. All supplier agreement should cover the information security requirements to ensure that the supplier employs enough controls in place to ensure the confidentiality, integrity and availability of information they store or process. All exceptions can be approved by the supplier security policy owner and/or the head of the department who owns the contract.

1.2. This Security Requirements to the Agreement sets forth the security requirements to be fulfilled by Supplier in relation to services provided under this document, including the Supplied Services.

1.3. The Director of IT is responsible for implementation and management of this procedure.

2. REVISION AND APPROVAL

Rev.	Date	Nature of Changes	Approved By
[Rev Number]	[Date of Issue]	Original issue.	[Procedure Approver Name]
1	12/27/2018	New procedure for New ISO 27001:2013 implementation	Director of IS
2.0	9/16/2019	Streamlined the supplier relationship policy to adhere to our environment	Director of IS

3. POLICY OVERVIEW

3.1. The Supplier shall ensure that any service provided by the Supplier under this Agreement, including the Supplied Services, has adequate security protection measures in order to manage threats. In the provision of such services, security protection shall be included which, at a minimum, meets the requirements of the Agreement.

3.2. The Supplier's undertakings regarding security protection measures include, but are not limited to, the following:

a) Supplier shall ensure that security systems and administrative tools are not used for any other purposes than intended;

b) Supplier shall not and will not introduce/remove/change security measures that have been implemented or ordered by Unical Aviation, without obtaining Unical Aviation's prior written approval.

3.3. The Supplier should appoint a point of contact. This person shall be responsible for liaising with Unical Aviation regarding all matters relating to security.

3.4. The Supplier can, upon Unical Aviation's request, provide Unical Aviation with a written report on how these security requirements are being met.

4. Security Operations

4.1. The Supplier shall ensure that Unical Aviation proprietary information and operational system state can be recovered following a Disaster or media failure.

4.2. If physical media containing Confidential Information and/or Unical Aviation Data is to be decommissioned or returned to Unical Aviation shall be made in a secure manner and any destruction shall be made in a way so that the information cannot be recreated or accessed. The Supplier shall have documented routines in place regarding destruction of physical media and shall be able to show proof of such destruction upon request.

5. Security logs and monitoring

5.1. The supplier should monitor the services provided to detect any deviation from its access control and should have a documented routine in place for log review and analysis in order to identify intrusion attempts.

6. Malware protection

6.1. The Supplier should always ensure that adequate and up to date malware protection exists and is implemented. Malware includes computer viruses, worms, Trojan horses, spyware, adware, and other malicious objects.

6.2. Malware protection should be implemented and updated.

7. Security patches

7.1. The Supplier should ensure that all critical security patches that are relevant for all software in operational use should be implemented no later than sixty (60) days after patch release date.

8. Intrusion Prevention System or equivalent solution

8.1. The Supplier should always ensure that an adequate and up to date intrusion prevention system, or equivalent solution, is installed.

8.2. The intrusion prevention system, or equivalent solution, should be implemented and updated according to a documented routine.

9. Communication over internal and public networks

9.1. The Supplier shall ensure that any non-public network utilized by the Supplier is protected in such a manner that only authorized access is possible.

9.2. The Supplier shall ensure that when public networks (Internet) are utilized by the Supplier, appropriate security mechanisms are in place so that no unauthorized access is possible

9.3. The Supplier should ensure that when Confidential Information or Unical Aviation Data is communicated over a public network, shall be secured and encrypted.

10. Software Development

10.1. In case the Supplier develops software or other services utilized by Unical Aviation, the Supplier shall adhere to a security software development lifecycle to prevent errors, loss, unauthorized modification or misuse of information in application

10.2. Software shall be tested for security vulnerabilities.

11. Business Continuity Plan

11.1. The Supplier should have an adequate and well documented business continuity plan in place in order to fulfill its undertakings towards Unical Aviation. The business continuity plan should be shown to Unical Aviation upon request.

12. Monitoring and Review of Supplier Services

12.1. Unical Aviation shall regularly monitor and review the services provided to ensure timely delivery of goods and services and remediate any issues that may occur with regards to quality.

12.2. This is in accordance with A.15.2.1

13. Managing Changes to Supplier Services

13.1. Any changes to services provided by suppliers must be managed in a way to ensure that risk is limited, and business processes, systems or information are not impacted greatly.

13.2. This is in accordance with A.15.2.2

14. Policy Compliance

14.1. Compliance Measurement

14.1.1. The IT Security team will verify compliance to this policy through various methods, including but not limited to, business tools reports, internal and external audits, and feedback to the policy owner.

14.2. Exceptions

14.2.1. Any exception to the policy must be approved by the IT Security team in advance.

15. Related References:

ISO27001:2017
NIST 800-171
Master Document list