Axway Security Statement
Information Security Management System Description

© Axway, May 27, 2020

imagination takes shape

As a leader in hybrid integration and content collaboration specializing in governing the flow of data, Axway is dedicated to safeguarding our customers' privacy and security. We provide end-to-end protection in highly-scalable, highly-available solutions and environments, because at Axway we understand that delivering secure systems is instrumental in sustaining trust, and by devising security policies that are transparent.

Axway can provide customers with a greater understanding of how their information is kept safe. With strict operational controls, customers can rest assured that personnel handling, viewing, and monitoring sensitive data have been properly trained and vetted through rigorous screening and quality checks. By layering granular, refined controls, Axway additionally helps protect organizations from the legal liabilities of inappropriate use, access, and viewing.

Our Information Security Approach

Axway relies on defined security processes when managing customer information.

Axway has chosen to establish, implement, maintain and continually improve an Information Security Management System which follows the International Code of Practice for Information Security Management, ISO/IEC 27001:2013.

ISO/IEC 27001 is an internationally recognized set of standards and controls used by organizations to preserve the confidentiality, integrity and availability of sensitive customer information. Axway is an ISO/IEC 27001:2013 certified entity demonstrating strict adherence to this framework.

As part of Axway's commitment to ensuring the security and integrity of information transmitted through and stored within its systems, Axway provides:

- Significant transparency related to its control environment
- Third-party certifications and attestations which customers can rely on to understand the details of Axway's control environment
- Third-party assurances that Axway has implemented these controls effectively

Additionally, Axway Leverages Information Technology Infrastructure Library (ITIL) based processes for incident and change management procedures. This allows Axway to better plan, execute, monitor and adjust business operations as needed

Our Information Security Management System

Axway maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Axway's business; (b) the amount of resources available to Axway; (c) the type of information that Axway will store; and (d) the need for security and confidentiality of such information.

Axway's security program is designed to:

- Protect the confidentiality, integrity, and availability of Customer Data or Professional Services Data in Axway's possession or control or to which Axway has access;

- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data or Professional Services Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data or Professional Services Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data or Professional Services Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Axway may be regulated.

Disclaimer

This document only applies to Axway. The security measures described herein are current as of May 27th, 2020 and are subject to change as Axway continues to improve the security of its systems and environments.

This document is provided for information only to our customers and does not constitutes any contractual commitment. More specifically, this document is not a statement that Axway is or will be ISO 27001 certified besides Axway Managed Cloud Services.

Without limiting the generality of the foregoing, Axway's Information Security Management System includes:

1. **Security Awareness and Training.** A mandatory security awareness and training program for all members of Axway's workforce (including management), which includes:
   a) Training on how to implement and comply with its Information Security Program;
   b) Promoting a culture of security awareness through periodic communications from senior management with employees.

2. **Access Controls**. Policies, procedures, and logical controls:
   a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
   b) To prevent those workforce members and others who should not have access from obtaining access; and
   c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the production data center or the facility housing Axway's servers, if applicable, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include:
   a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
   b) Camera surveillance systems at critical internal and external entry points to the data center;
   c) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
   d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any Security Breach. Such procedures include:
   a) Roles and responsibilities: formation of an internal incident response team with a response leader;
   b) Investigation: assessing the risk the incident poses and determining who may be affected;
   c) Communication: internal reporting as well as a notification process in the event of unauthorized disclosure of Customer Data or Professional Services Data;
   d) Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and
   e) Audit: conducting and documenting root cause analysis and remediation plan.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Customer Data or production systems that contain Customer Data. Such procedures include:
   a) Data Backups: A policy for performing periodic backups of production file systems and databases on Axway's servers, as applicable, according to a defined schedule;
   b) Disaster Recovery: A formal disaster recovery plan for the production data center, including:

   i) Requirements for the disaster plan to be tested on a regular basis, currently once a year; and
   ii) A documented executive summary of the Disaster Recovery testing.
c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed to minimize the loss of vital resources.

6. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Data and protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Customer Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Customer Data stored on desktops, laptops or other removable storage devices.

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Customer Data, considering available technology so that Customer Data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including:
    a) Designating a security official with overall responsibility;
    b) Defining security roles and responsibilities for individuals with security responsibilities; and
    c) Designating a Security Committee consisting of cross-functional management representatives to meet on a regular basis.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Where applicable, such testing includes:
    a) Internal risk assessments;
    b) ISO 27001 certifications for Cloud Managed Services environment; and
    c) Service Organization Control 2 (SOC2) audit reports (or industry-standard successor reports) for Cloud Managed Services.

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:
    a) Reviewing changes affecting systems handling authentication, authorization, and auditing;
    b) Reviewing privileged access to Axway production systems; and
    c) Performing network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Axway makes to production systems, applications, and databases. Such policies and procedures include:
    a) A process for documenting, testing and approving the patching and maintenance of the Services;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis.

14. Program Adjustments. Axway monitors, evaluates, and adjusts, as appropriate, the security program considering:

a) Any relevant changes in technology and any internal or external threats to Axway or the Customer Data;
b) Security and data privacy regulations applicable to Axway; and
c) Axway's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

15. Devices. All laptop and desktop computing devices utilized by Axway and any subcontractors when accessing Customer Data:

a) will be equipped with a minimum of AES 128-bit full hard disk drive encryption;
b) will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and
c) shall maintain virus and malware detection and prevention software to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by supplier of such software.