Security Appendix

4.11.2024

Posti security requirements for suppliers and deliveries

Contents

1. Introduction 3

2. General cyber security measures for suppliers 4

3. Delivery specific cyber security requirements 5

3.1. Basic principles & scope 5

3.2. Right to audit 5

3.3. Security & risk management 6

3.4. Personnel security 6

3.5. Asset management 6

3.6. Access control 7

3.7. Data protection 7

3.8. Physical security & working at Posti premises 7

3.9. Operations security 8

3.10. Network security 8

3.11. Integrating into Posti processes and systems 8

3.12. Security & privacy by design in system development 9

3.13. Incident management 9

3.14. Business continuity 9

3.15. Data privacy 10

Glossary 11

1. Introduction

Posti Group Oyj ("Posti") relies heavily on its data and especially personal data of Posti's customers that Posti processes (hereby referred to as "Posti Information"), to successfully deliver its services. Therefore, it is essential that the confidentiality, integrity, and availability of information and related services are secured.

Any third party (referred from now on as "Supplier") that has access to, processes, or stores Posti information must adhere to this document to ensure that Posti maintains the trust of all its stakeholders and remains compliant with legal and regulatory requirements.

Suppliers may have access to a wide range of Posti systems, services, or information. This access could be either through storing information or infrastructure belonging to Posti at an offsite facility (e.g. as part of a cloud service provider arrangement), or through having remote or physical access to Posti's systems. As a result, all applicable security controls must be implemented according to applicable standards and risks managed in co-operation with Posti.

The purpose of this document is to ensure that Posti's information and systems that are accessed by Suppliers are subject to appropriate protection based on applicable security controls. Posti expects Suppliers to report identified risks, detected security incidents, and be proactive in building in security to service or product in scope of the agreement.

Requirements shared in this document are divided into two sections:

- **General cyber security measures for suppliers**
  This section describes a set of cyber security measures that each supplier needs to adhere in their operations based on risk and relevance to supplier

- **Delivery specific cyber security requirements**
  This section describes cyber security requirements, that must be considered based on risk and relevance while delivering products, systems, or services to Posti.

2. General cyber security measures for suppliers

This section describes a set of cyber security measures that all suppliers to the Posti are expected to adhere to the extent relevant on their cyber security risk posture.

The listed cyber security measures are implemented in Posti to mitigate cyber security risks to an acceptable level and to maintain regulatory compliance. Supplier is expected to implement risk-based cyber security measures to ensure regulatory compliance and to mitigate cyber risks potentially having an impact on Posti.

The measures shall be based on aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

1. Policies and procedures on risk analysis and information security. The supplier shall demonstrate an acceptable level of adherence to industry best practices (e.g., ISO27k, NIST CSF, ISF Standard of Good Practices).
2. Policies and procedures for handling security incidents and reporting to Posti about incidents impacting data or operations related to Posti.
3. Policies and procedures on business continuity, such as backup management and disaster recovery, and crisis management. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
4. Plans and activities on supply chain security. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.
5. Policies and procedures on security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.
6. Policies and procedures for evaluating the effectiveness of cyber security risk-based measures.
7. Plans and activities for basic cyber security hygiene practices and training.
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
9. Policies and procedures on human resources security, access control and asset management.
10. Policies and procedures on the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

3. Delivery specific cyber security requirements

3.1. Basic principles & scope

a) Applicable legal and regulatory requirements (e.g. GDPR – General Data Protection Regulation) must always be adhered to when they apply.

b) The supplier must nominate an individual(s) who acts as the primary point(s) of contact for Posti in situations where information security and privacy are concerned.

c) In all cases where Subcontractors are used by the Supplier, the Supplier is fully liable for their performance. Supplier is responsible in ensuring the compliance of respective security measures also for possible Subcontractors used to deliver services to Posti. Before transferring production of services to a Subcontractor, use of the Subcontractor and its security arrangements and measures must be approved by Posti to the extent they differ from similar used by the Supplier. For example, any data transfers outside EU/ETA must be approved by Posti.

d) As an assumption, no payment card cardholder data is stored, transmitted, or handled as part of the Services, unless otherwise agreed in the main contract, in which case PCI-DSS requirements must be fulfilled.

e) Posti-specific requirements are detailed in this document and may be further defined in contracts. In case there are requirements in this document that the Supplier cannot adhere to, Posti shall be notified without delay. Posti and Supplier shall then agree, if deemed necessary, complementary controls to address potential risks posed by non-compliance. It should be noted that notification of non-compliance does not lessen the Supplier's responsibilities towards potential breaches of contract.

f) Supplier shall regularly conduct independent reviews and assessments of security level and the implementation of security measures in its organization and processes related to the delivery. The result and findings and the required corrective measures are to be discussed with Posti as part of the service governance model.

3.2. Right to audit

a) To ensure compliance with Posti security requirements, Posti (or a third party on behalf of Posti) may carry out an information security and privacy assessment or an audit to the Supplier and a Subcontractor used by Supplier. Supplier must assist Posti with the provision of any relevant documentation requested and provide access to all relevant sites, as is necessary and when reasonably requested by Posti.

b) Supplier's information security practices and compliancy with requirements can be evaluated with information security self-assessments by the Supplier.

3.3. Security & risk management

a) Monitoring and evaluation of information security and privacy related topics regarding the delivery must be covered by a separately agreed approach between the Supplier and Posti.

b) Supplier must maintain a register of any identified security risks related to the delivery. Identified risks must be communicated to Posti.

3.4. Personnel security

a) If Posti requests, Supplier is responsible that security clearances and/or background checks, as allowed by the local law, are conducted on Supplier Personnel (or supplier's subcontractors) involved in the delivery.

b) Non-disclosure agreement shall be put in place with all Supplier employees who have access to Posti's Information and the delivery.

c) Supplier must make sure that key persons and roles associated with the delivery are identified and deputy arrangements established in case of absences. Supplier must inform Posti if changes take place in key personnel involved in the delivery.

d) Supplier must provide information security and privacy awareness training to all Supplier employees (including subcontractors) involved in the delivery. For Suppliers providing software development for Posti, secure development training should be provided similarly as to Posti's internal software developers.

3.5. Asset management

a) The Supplier must record in an asset inventory all assets that are used to process or store Posti Information as part of the delivery. The inventory must be maintained and kept up to date and all assets must have a designated owner. The Supplier should use Posti assets and resources (e.g. email, IT systems, platforms, networks, cloud, external services, etc.) when relevant.

b) If not separately specified, all assets received from Posti must be treated as confidential.

c) Posti data, material or systems that are owned or leased by Posti, must not be used without a written specific permission from Posti to any other purposes other than those specified in the Service Agreement between Posti and the Supplier (e.g. used for system development and testing). A thorough assessment on impact regarding privacy, security and changes in risks are required before Posti can provide such a permission.

d) Supplier must securely and permanently destroy/wipe Posti Information from all media and/or devices when it is no longer required for the delivery. Supplier must ensure that also automatic backup arrangements are considered prior to disposal of Posti Information. At Posti's request or upon termination of Service agreement, Supplier must return to Posti, without delay, information, and materials owned or managed by Posti which were acquired during the Service lifecycle.

3.6. Access control

a) Supplier must ensure that only relevant personnel have access to Posti systems and information, or Supplier systems used in delivering the service and potentially used in processing or storing sensitive Posti data (incl. data of Posti's customers). Supplier must maintain and review an up-to-date list of all personnel who are authorized to access Posti assets and resources.

b) Supplier must ensure that multi-factor authentication, based on Posti approved remote access methods, is used when accessing Posti Information, networks, systems, and services.

3.7. Data protection

a) Data transfer methods, potentially including encryption, between Supplier and Posti must be mutually agreed. When communicating with Posti by email, the Supplier shall use Posti email account for external collaborators when relevant.

b) Supplier shall have means to encrypt Posti's sensitive data at rest and in transit.

3.8. Physical security & working at Posti premises

a) Supplier must ensure that all personnel present in premises where Posti Service is delivered, are authorized.

b) If work related to the delivery is conducted remotely outside Supplier or Posti premises, secure remote working practices must be in place and followed by Supplier personnel.

c) When Supplier is working in Posti's facilities, all Supplier's Personnel must adhere to the local rules of the Posti facility or area in question.

d) Posti assets, material and equipment shall not be removed from the premises without separate permission from Posti.

3.9. Operations security

a) Procedures for operational activities to provide the Services to Posti must be documented, maintained, and made available to anyone responsible for managing, administering, or developing applications or systems used to process or store Posti's Information.

b) Any changes to the organization, business processes, or systems processing Posti's information that affect information security or privacy must be controlled, documented, and authorized through a formal process. Any such changes must be reviewed and tested to ensure that there is no adverse impact on services provided to Posti or to the security of Posti's or Posti's customers' Information.

c) Supplier used development/test and production facilities processing Posti's Information must be separated from each other to reduce the risk of unauthorized access or changes to the operational environment or Posti.

d) Development and test environments should use only test data or pseudonymization to protect sensitive data and if this is not possible, a risk needs to be documented, evaluated, and addressed in cooperation with Posti and the Supplier.

e) Back-up processes should be in place and tested for timely recovery of systems used in providing the service to Posti.

3.10. Network security

a) As a principle, no Posti Information should be copied outside Posti control. If this is required, a risk needs to be documented, evaluated, and addressed in cooperation with Posti and the Supplier.

b) Any security testing and scanning of Posti assets may not be done without permission from Posti.

c) Access to Posti networks, connectivity, and maintenance connections must be separately agreed and arranged with applicable security measures.

3.11. Integrating into Posti processes and systems

a) Supplier must validate the integrity of products or systems by performing appropriate security scanning and testing before possible integration into Posti's infrastructure.

b) For authorization and access management, Suppliers shall integrate to Posti AD (Active Directory) as well as Posti access management procedures, where possible. If this is not possible, a risk needs to be documented, evaluated, and addressed in cooperation with Posti and the Supplier.

c) Supplier systems integrated to Posti systems, shall also integrate, where possible and justified, to Posti SOC (Security Operations Center) for the purposes of security monitoring. In cases where this is not possible, a risk needs to be documented, evaluated, and addressed in cooperation with Posti and the Supplier.

3.12. Security & privacy by design in system development

a) Supplier must design and implement all Products and Services delivered to Posti by considering privacy and security aspects (e.g. privacy and security by design) and adhere to applicable legal, statutory, or regulatory compliance obligations.

b) Services, products, and systems must be designed, developed, tested, deployed, and maintained in accordance with leading industry standards (e.g. OWASP Top 10 for Web Applications and OWASP Application Security Verification Standard).

c) Posti secure software development life cycle, secure software development principles and practices must be followed.

3.13. Incident management

a) Any breach or suspected breach of security or privacy, such as compromise of Posti Information or systems, must be reported to Posti without delay. Subject to possible restrictions by law, Posti has the right to take part in investigations or incident handling when Posti's interests are endangered.

Supplier must deliver the report of the security incident investigation as well as the root cause analysis with suggestions for corrective actions to be taken to remediate the situation for Posti. The results and needed measures to be taken including prioritization are discussed as part of the service governance model.

Contact details for reporting security incidents:

ICT Service Desk
phone: +358 20 451 4433
email: ictservicedesk@posti.com

or in non-urgent matters

email: information.security@posti.com

3.14. Business continuity

a) Posti must assure by law its services during all national or local disturbances or emergencies. Supplier must take actions (regarding people, locations, assets, communication, and information systems etc.) so that the services provided, and which are critical for Posti's provision of its services, can timely recover from possible incidents in all circumstances.

b) Supplier must have business continuity and disaster recovery plans in place to minimize the impact of realized risk events on the Supplier organization and potential Subcontractors involved in the production of services to Posti.

c) The plans must at minimum address:

   1. how business operations will be restored following an interruption to or failure of business processes within an agreed time period, accepted by Posti, and how information security will be maintained
   2. define arrangements to inform and engage relevant Posti personnel in their execution
   3. regular testing, review and updating of the plans

d) The availability and continuity related requirements (e.g. Maximum Tolerable Downtime, Recovery Point Objective, and Recovery Time Objective) for the Service provided to Posti are to be agreed together between Posti and the Supplier.

3.15. Data privacy

a) When personal data is processed, the Supplier (and possible subcontractors) shall have a formal, documented, comprehensive and accurate record of processing activities (ROPA) based on a data mapping exercise that is regularly reviewed, according to the Article 30 of the GDPR.

b) If the Supplier processes personal data on behalf of Posti, a separate Data Processing Agreement (DPA) shall be signed between Posti and the Supplier.

c) No personal data of Posti employees or Posti’s customers that the Supplier is a processor or the controller of, shall be transferred outside of the European Union (EU) and to countries that the European authorities have not deemed to have adequate safeguards in place to protect the data without consent from Posti.

Glossary

Term	Description
Active Directory (AD)	A directory service developed by Microsoft for Windows domain networks
Data Processing Agreement (DPA)	A legally binding contract that states the rights and obligations of each party concerning the protection of personal data
General Data Protection Regulation (GDPR)	Regulation in EU law considering data protection and privacy.
Information Security Forum (ISF)	An international information security best practices organization
ISO27k	The ISO/IEC 27000-series information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
Multi-Factor Authentication (MFA)	An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism
NIST CSF	NIST Cybersecurity Framework is a guidance on how both internal and external stakeholders of organizations can manage and reduce cybersecurity risk. NIST CSF is published by US National Institute of Standards and Technology.
OWASP	The Open Web Application Security Project, is a non-profit online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.
Posti information	All data controlled by or processed at Posti
Record of processing activities (ROPA)	Record of processing activities is a written description of organization's personal data processing.
Security Operations Center (SOC)	Posti's centralized unit that deals with security issues on an organizational and technical level.
Supplier / Third-party	Refers to Posti clients and external suppliers, including organizations or individuals contracted by Posti to use, handle or process Posti information.