Productsup Group

Information Security Policy Summary

Version 1.0

Table of Contents

1.0 Common Policy Elements

1.1 Purpose and Scope

Information is a valuable asset that must be protected from unauthorized disclosure, modification, use or destruction. Prudent steps must be taken to ensure that its confidentiality, integrity and availability are not compromised. This document provides an overview over a uniform set of information security policies for using the Products Up GmbH (hereafter referred to as “Productsup”) technology resources. In addition to defining roles and responsibilities, information security policies increase users’ awareness of the potential risks associated with access to and use of technology resources. Employee awareness through dissemination of these policies helps accelerate the development of new application systems and ensure the consistent implementation of controls for information systems. Productsup’s information security policies are based upon the internationally accepted ISO 27001:2013 information security standard framework. The standards will be considered minimum requirements for providing a secure environment for developing, implementing and supporting information technology and systems.

1.2 Enforcement

These policies must be adhered to by all Productsup departments, divisions and enterprises (hereafter referred to as “departments”) unless specifically granted an exception. Individual departments may develop more detailed procedures to handle department-specific cases, provided they adhere to the policies that they support. This policy will guide annual security reviews by the Information Security Team, as well as audits by a designated third party as requested by Productsup. Violators of these policies may be subject to employee disciplinary procedures as described in the Productsup’s Human Resources Policies. Departments and divisions may impose sanctions upon their employees, within accepted guidelines, for violations of these standards

1.3 Exceptions

Exceptions to information security policies must be approved by the Information Security Team with a review. In each case, the department or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. If approved, exceptions will be documented.

2.0 Information Security

2.1 Policy

2.1.1 Information Security Commitment Statement

2.1.1.1 Information is a valuable Productsup asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies and procedures must be implemented to ensure that the integrity, confidentiality and availability of Productsup information are not compromised.

2.1.2 Security Responsibility, Review and Evaluation

2.1.2.1 Technology Resources is responsible for establishing and managing the security of all systems. Technology Resources will as needed but at a minimum on an annual basis review the most current best practices regarding the use of technology and will amend and/or issue new policies, procedures, and/or controls to reflect the most appropriate solution for security of Productsup information.

2.1.3 User Responsibility

2.1.3.1 Productsup technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties in a secure electronic environment. The use of such resources imposes certain responsibilities and obligations on users and is subject to all applicable Productsup policies. It is the responsibility of every user to ensure that such resources are not misused and to adhere to all Productsup security policies and procedures, which are located in the Information Security Space on Productsup's Confluence Instance.

3.0 Risk Assessment and Treatment

3.1 Assessing Security Risks

3.1.1 Risk Assessments

3.1.1.1 Risk assessments will be performed annually to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur.

3.1.1.2 Risk assessments will be undertaken in a methodical manner capable of producing comparable and reproducible results.

3.1.1.3 Risk assessments will have a clearly defined scope in order to be effective.

3.1.1.4 The outcome of a risk assessment will be a report defining and prioritizing risks, based on threats and vulnerabilities and impact to Productsup information.

4.0 Organizational Security

4.1.1 Management Commitment to Information Security

4.1.1.1 Productsup is fully committed to actively supporting security within the organization through clear direction, demonstrated commitment, explicit assignment, acknowledgment of information security responsibilities, and the support of a Information Security Steering Committee developed to provide Governance for all Information Technology policies and procedures.

4.1.1.2 The Information Security Steering Committee will be composed of appointed executive leaders and will meet, at a minimum, on a bi-annual basis. The committee will:

- review and approve information security policy;
- provide clear direction and visible management support for security initiatives;
- approve the resources needed for information security;
- approve assignment of specific roles and responsibilities for information security across Productsup;
- approve plans and programs to maintain information security awareness;
- and ensure that the implementation of information security controls is coordinated across Productsup.

4.1.2 Independent Review

4.1.2.1 Productsup's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) in accordance with the ISO27001 standard will be reviewed on an annual basis.

4.1.2.2 Such a review will be carried out both internally and by individuals independent of the area under review such as a third party organization specializing in such reviews. Individuals carrying out these reviews must have the appropriate skills and experience.

5.0 Asset Classification and Control

5.1 Accountability for Assets

5.1.1 Ownership of Assets

5.1.1.1 All information and assets associated with information processing will be owned by a designated Productsup staff member. The asset owner will be responsible for:

- ensuring that information and assets associated with information processing facilities are appropriately classified;
- and defining, providing, and reviewing access restrictions and classifications, taking into account applicable access control policies.

5.1.2 Acceptable Use of Assets

5.1.2.1 Productsup resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to Productsup policies. It is the responsibility of each user to understand and abide by Productsup's Acceptable Use Policy and to ensure that such resources are
not misused

5.1.2.3 Productsup reserves the right to retrieve and read any data composed, transmitted or received through inbound/outbound connections and/or stored on Productsup systems.

5.1.3 Information Classification

5.1.3.1 All Productsup information and information entrusted to Productsup from outside agencies fall into one of four sensitivity classifications. Public, Internal, Confidential, Top-Secret.

5.1.3.2. Based on the information sensitivity, specific requirements may apply for labeling, handling, transfer and destruction.

6.0 Human Resources Security

6.1 Prior to Employment

6.1.1 Screening / Terms of Employment

6.1.1.1 Qualification and identity checks will be conducted on all Productsup employees and contractors.

6.1.1.2 The terms of employment specify obligations for secrecy and data privacy.

6.2 During Employment

6.2.1. Responsibilities and Awareness

6.2.1.1 All employees will be required to complete annual training on information security awareness and concepts.

6.2.1.2 All employees will practice security awareness and remain vigilant against fraudulent activities.

6.2.1.3. All employees will immediately report incidents involving any Productsup information to the Information Security Team.

6.2.1.4 All employees will note and report observed or suspected security weaknesses to systems and services directly to the Information Security Team.

6.3 Termination or Change of Employment

6.3.1 Responsibilities for performing employment termination or changes of employment are defined in Productsup's HR procedures.

6.3.2 Human Resources is responsible for the overall termination process and will coordinate with the manager of the person terminating and the Internal IT to manage the access aspects of the relevant procedures.

6.3.3 All employees, contractors, and third party users must return all of the Productsup's assets in their possession upon termination of their employment, contract, or agreement.

6.3.4 The access rights of all employees and third party users to information and information processing facilities must be removed upon termination of their employment, contract, or agreement, or adjusted as necessary upon any change in employment.

7.0 Physical and Environmental Security

7.1 Secure Areas

7.1.1 Physical Security Perimeter

7.1.1.1 A security assessment of all key information processing facilities will be performed annually to assess their physical security.

7.1.2 Physical Entry Controls

7.1.2.1 Access to any Productsup data center, network operations center, telecommunications or other similar information processing facility will be restricted and physically controlled.

7.1.2.2 Access to any office, computer room, or work area that contains confidential information will be physically restricted.

7.2 Equipment Security

7.2.1 Equipment Location and Protection

7.2.1.1 Production systems, including, but not limited to servers, network equipment, and telephony systems will be located within a physically-secured area.

7.2.1.2 Appropriate precautions including removing or encrypting sensitive or confidential data will be taken when sending equipment off site for maintenance.

7.2.2 Secure Disposal or Re-use of Equipment

7.2.2.1 Prior to approved disposal, media containing confidential information must be destroyed to render the information unrecoverable.

7.2.2.2 All hardcopy materials that contain confidential information must be shredded.

8.0 Asset Management

8.1 Media Handling

8.1.1 Management of Removable Media

8.1.1.1 If no longer required and not under public records requirements, the contents of any re-usable media that are to be removed from the organization will be made unrecoverable.

8.1.1.2 Where necessary authorization will be required for media removed from Productsup and a record of such removals will be kept in order to maintain an audit trail.

8.1.1.3 All media will be stored in a safe, secure environment, in accordance with manufacturers' specifications.

8.1.2 Disposal of Media

8.1.2.1 When media is worn, damaged or otherwise no longer required,it will be disposed of in a secure manner. To prevent the compromise of confidential information through careless or inadequate disposal of computer media, formal procedures will be established for secure media disposal.

8.2 Access to Systems

8.2.1 Publicly-Accessible System

8.2.1.1 The dissemination methods for Productsup's information classified as public will have, at a minimum, protection from unauthorized modification and denial of service attacks.

8.2.1.2 Consideration of security controls that will be applied to publicly-available systems will include the following:

- Information to be disseminated is classified in compliance with data protection legislation
- Confidential information must be protected during the collection process and when stored
- Access to the public system does not allow unauthorized access to networks to which it is connected.
- Productsup information classified as other than public will not reside on systems where public information is being served.

8.3 Backup & Recovery

8.3.1 Backup Requirements

8.3.1.1 Backup procedures will be existent for all business critical systems and application to minimize loss of data in case of an incident or outtage.

8.3.1.2 Backup recovery procedures will be regularly tested to ensure backups are operational when required.

8.3.1.3 Backups must be encrypted where confidential data is involved.

9.0 Access Control

9.1 Business Requirement for Access Control

9.1.1 Access Control Policy

9.1.1.1 All confidential information will be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

9.1.1.2 Access control procedures will control access based on the need to know / least privilege.

9.1.1.3 All information possessed by or used by a particular Productsup unit will have a designated owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

9.1.1.5 The authority to grant access to Productsup information will be provided in writing, only by the owner of the information or their designate.

9.1.1.6 Default access privileges will be set to “deny-all” prior to any specific permissions being granted.

9.1.1.7 Unless it has specifically been classified as public, all Productsup information will be protected from disclosure. If non-public information is compromised or suspected of being compromised, the information owner and the appropriate security administration will be notified immediately.

9.1.1.8 User access reviews shall be conducted and documented on a quarterly basis to ensure access rights are appropriately assigned to users across all systems and applications.

9.2 User Access Management

9.2.1 Access Authorization

9.2.1.1 User IDs may be granted to specific users only when approved in advance by the user's management.

9.2.1.2 Prior to being granted to users, application system privileges will be approved by the involved application system owner.

9.2.1.3 Without specific formal approval from the user's management, administrators will not grant system privileges to any user.

9.2.2 Clear Desk and Screen Policy

9.2.2.1 Departments that process confidential information will consider adopting a clear desk policy for paper and removal storage media and a clear screen policy, in order to minimize the risks of unauthorized access to and loss of such information, both during and after normal working hours.

9.2.2.2 Computers and mobile devices that access or use confidential data will be protected by password-protected screensavers when unattended.

9.2.2.3 Sensitive or confidential information will be removed from printers and facsimile machines immediately upon printing.

9.2.2.4 The use of power-on passwords will be required where the Computer or any device that contains confidential information.

10 Cryptographic Controls

10.1 Requirements for use of cryptography

10.1.1 Encryption in Transit

10.1.1.1 All data exchanged through the internet will be encrypted in transit using modern encryption algorithms.

10.1.2. Encryption at Rest

10.1.2.1 Servers holding sensitive data will be encrypted at rest where possible.

10.1.2.2 All laptops and or personal computers used by employees for Productsup will be encrypted.

10.1.2.3 Backups will always be encrypted either before transfer or using a technique offered by the provider where the backup is stored (for example Amazon S3 Server-Side-Encryption).

11.0 Information Security Incident Management

11.1 Reporting Information Security Events and Weaknesses

11.1.1 Reporting Security Incidents

11.1.1.1 Any suspected or observed breaches of confidential or restricted information must be reported to the Information Security Team.

11.2 Management of Information Security Incidents and Improvements

11.2.1 Responsibilities and Processes

11.2.1.1 It is the responsibility of all management staff to be familiar with the incident management process.

11.2.2 Collection of Evidence / Learning from Incidents

11.2.2.1 All collection and presentation of evidence will be in compliance with the incident management process.

11.2.2.2 The information gained from the evaluation of information security incidents will be used to identify recurring or high impact incidents.

12.0 Compliance

12.1 Compliance with Legal Requirements

12.1.1 Identification of Compliance Areas

12.1.1.1 Resources has been assigned responsibility for the establishment of Productsup-wide information security policies. However, each department is responsible for developing its own specific procedures necessary to ensure operational compliance with internal provisions and external legal and regulatory requirements.

12.1.1.2 The information processing resources of Productsup are provided for the business purposes of Productsup.

12.1.1.3 Compliance with data protection legislation requires appropriate management control. The owner of such data is responsible for ensuring awareness of the data protection requirements defined in the relevant legislation.

12.2 Compliance with Security Policies and Standards, and Technical Compliance

11.2.1 Identification of Compliance Areas

11.2.1.1 Productsup information systems will submit to regular reviews of technical security audits. These reviews will be performed annually to measure compliance with existing security implementation standards. Technical compliance evaluations are based on performing various types of tests and examining configurations.

11.2.1.2 Compliance testing will identify weaknesses subject to exploitation, and qualify results as to the nature of criticality. Technical evaluations will be done in cooperation with operations personnel to avoid impact on production environments.

11.2.1.3 The handling of results and data obtained in such evaluations will be handled as confidential information.