Information Security Policy

For Unit4 Global SaaS Operations

Information Security Policy

For Unit4 SaaS Operations

Summary

The execution of business processes within Unit4 Global SaaS Ops is based on information obtained from information systems that may or may not be automated. Good progress of the business processes and the organization's survival are therefore increasingly dependent upon the reliability of the information and the information systems in which this information is processed. Unit4 Global SaaS Ops has an interest in an adequate level of information security, not just for its own operational management. Customers, suppliers and supervisory authorities also make high demands of the reliability of the information provision of Unit4 Global SaaS. Insufficient information security at Unit4 Global SaaS Ops can lead to unacceptable risks when executing the processes. Incidents and violations of these processes can lead to large financial consequences and damage of reputation. Not just for Unit4 Global SaaS Ops itself, but also for Customers as they have entrusted Unit4 Global SaaS Ops with their information. The necessity to systematically address the security of the information provision is therefore extremely great.

The implementation of the Information Security Policy ensures that, within Unit4 Global SaaS, insight will be developed into the organizational value of the information regarding the execution of the processes, and the dependencies and vulnerabilities of the processing and the underlying information systems. The insight into these risks enables a proper consideration to be made regarding the measures necessary to limit these risks.

Unit4 Global SaaS Ops uses the following definition of information security – The total of standards, plans and measures to guarantee the availability, confidentiality and integrity of the information provision within Unit4 Global SaaS Services.

The general objective of Unit4 Global SaaS Ops' Information Security Policy is the establishment, recording and communication of objectives, key points and preconditions of Unit4 Global SaaS Ops with regard to the security of the information provision.

- The Information Security Officer is responsible for upholding the policy, giving advice and guiding the implementation.
- Management is responsible for the information security measures that are implemented within their section of the organization (divisions, departments and supporting business sections).
- Line Management of these sections of the organization are primarily responsible for choosing, executing and upholding the information security measures.
- The Information Security Officer initiates policy-related activities, coordinates the introduction of the security measures and advises the responsible management.
- All employees are responsible for the correct execution and upholding of the Information Security Policy and related standards and procedures.

Compliance with the Information Security Policy will be checked regularly by means of internal audits.

All security incidents, both real and suspected, should be reported to the Information Security Officer, so that immediate action can be undertaken to limit potential damage to Unit4 Global SaaS Ops, its employees and its Customers, as far as that is possible.

Introduction

Unit4 Global SaaS Ops uses the following definition of information security: Information security is the total of standards, plans and measures to guarantee the availability, confidentiality and integrity of the information provision within Unit4 Global SaaS Services.

1. Importance of information security

   The execution of business processes within Unit4 Global SaaS Ops is based on information obtained from information systems that may or may not be automated. Good progress of the business processes and the organization's survival are therefore increasingly dependent upon the reliability of the information and the systems in which this information is processed.

   Unit4 Global SaaS Ops has an interest in an adequate level of information security, not just for its own operational management. Customers, suppliers and supervisory authorities also make high demands of the reliability of the information provision of Unit4 Global SaaS Services. Insufficient information security at Unit4 Global SaaS Ops can lead to unacceptable risks when executing the processes.

   Incidents and violations of these processes can lead to large financial consequences and damage of reputation. The necessity to systematically address the security of the information provision is therefore extremely great.

2. Quality aspects - Information security for the purpose of reliable information provision concerns the following quality aspects:
   a. Availability – The information is available when the organization needs it.
   b. Integrity – The information is completely accurate, up-to-date and verifiable.
   c. Confidentiality – The information is accessible only to the person with authorized access.

   Information security within Unit4 Global SaaS Ops is focused on both automated as well as non-automated information provision.

3. Objective – The objective of the Information Security Policy is :
   a. Clearly indicating what its objectives, key points and preconditions are.
   b. Clearly indicating who has what tasks, authority and responsibilities.

   The Information Security Policy constitutes the basis for clarifying to all employees and relevant external relations of Unit4 Global SaaS Ops what the Unit4 Global SaaS Services' Information Security Policy involves.

Objective, position and scope

The general objective of the Information Security Policy is: The establishment, recording and communication of objectives, key points and preconditions of Unit4 Global SaaS Ops with regard to the security of the information provision of Unit4's Global SaaS Services. Information security is based on three quality aspects:

- availability
- integrity
- confidentiality

Availability – Guaranteeing the availability of the information provision comprises of measures that ensure:

- continuity
- timeliness

Integrity - Guaranteeing the integrity of the information provision comprises of measures that, with regard to data, software and information distribution, ensure:

- accuracy and consistency
- validity
- completeness
- verifiability
- authenticity

Confidentiality - Guaranteeing the confidentiality of the information provision comprises of measures that ensure:

- Exclusivity of information: programs, data and equipment are only accessible for those who have explicitly been authorized for this.
- Protection of privacy when storing and using information.

Key points and preconditions

Within Unit4 Global SaaS Services, the ISO27001 (Code of Practice for Information Security) is determined as the standard in which the guidelines to be used for information security are recorded. The demands of the information security are recorded in the Standards Framework and should be specified for each section of the organization. The intended measures should be in agreement with these demands.

Rights to data collections and information systems

For each section of the organization, it has been established who the holder is for each data collection and each personal data register and therefore who has control over this data collection. The holder determines how the management of these data takes shape:

- Who has access to the data (authorizations).
- Who is authorized to consult, alter, remove or provide data to third parties.
- Who will monitor the constant integrity of the data collections and information systems.

Prior to the implementation, it is clear for all parties involved with each developed system who has ownership and where the system management will be performed.

Owners of information and information systems

Information systems or resources and data collections have an owner. Resources are, for example, applications, network infrastructures, data, desktops, laptops, mobile equipment, et cetera. The owner is responsible for the availability, the integrity and the confidentiality of the information, the information system or resource. This also applies to outsourcing.

Owners of information and information systems are responsible for:

- Determining the value and the importance of information and information systems.
- Classifying information and information systems.
- Evaluating the risks of the information provision, and identifying the necessary security measures.
- Guaranteeing that all security measures are implemented and that the implemented security measures are effective.
- Guaranteeing that personal data are treated in agreement compliance standards.

Note: the owner of information and the owner of the system processing this information can be two different people.

Information security is a line responsibility

Although the Information Security Officer establishes the Information Security Policy (strategically/tactically), it is the line's task to shape this further (tactically/operationally). The Line Managers are responsible for the correct execution of their instructed business processes, the associated information provision and for its proper functioning, and thereby also for the information security. The integral management has the primary responsibility for choosing, executing and upholding the information security measures.

Information provision is everyone's responsibility

The security philosophy of Unit4 Global SaaS Ops expects a duty of care and alertness from each employee. It is expected that everyone will act in agreement with the specified regulations, for example with regard to the use of passwords. Management is expected to encourage this conduct.

Information security is part of operational management

Information security is for Unit4 Global SaaS Ops, not an objective or policy per se, but an integral part of the business objectives and the management system of the operations. Correct security contributes to the business goals and to the reliable execution of the business processes. The aim should be optimum information security, whereby the following aspects play a role:

- The consequences in relation to compliance requirements of the data recorded and processed by Unit4 Global SaaS Ops.
- The necessity of minimizing the security risks and the security demands based on this.
- The desired level of efficiency and effectiveness of the information provision.
- The costs and the burdens of the information provision.

Handling information provision

Reliability requirement

The basis of the information security is formed by the set of standards (‘what’). These standards are subsequently translated, by the sections of the organization, into suitable, specific measures (‘how’). Every section of the organization is thus obliged to explicitly make a motivated statement about the desired security level and, by itself, identify measures based on classification and risk analysis. Every section of the organization should thereby, for its separate information systems, continually consider if the general level of security is appropriate, or if additional measures are necessary.

Risk analysis

Unit4 Global SaaS Ops perform cyclic risk analysis, whereby the threats to, effects on and vulnerability of the information systems and data, as well as the likelihood of these threats occurring, will be judged. Based on risk analysis, security measures are determined whereby a security level acceptable to Unit4 Global SaaS Ops is realized. In determining the measures, the costs and benefits of these measures are considered. With regard to performing risk analysis, Unit4 Global SaaS Ops uses the following key points:

- The business units perform their own risk analysis:
  - with the introduction of new information systems or important alterations,
  - following an extensive security incident,
  - at least once every three years for all company assets deployed for the most important business processes.
- The information resources and the implemented security measures are established and recorded.
- The risks are identified and the risk management strategy is recorded, for example:
  - avoiding risks
  - limiting risks

    - allocating risks in third parties
    - accepting risks
- Risks that can lead to a considerable financial loss, damage or other negative consequences for Unit4 Global SaaS Ops are not accepted without explicit agreement of the responsible management
- Risks accepted by the responsible management are reported to the Information Security Officer
- The process for performing risk analysis and the results of the risk analysis should be documented and approved by the responsible management for the business unit concerned.
- The results of the risk analysis, approved by the responsible management, are reported to the Information Security Officer.

Classification

A different need or necessity for security exists for different types of data. Requirements with regard to availability, confidentiality and integrity can be different depending on the type of data. In order to be able to draw up and apply security requirements for every type of data, data has to be classified. The application Product Manager is responsible for classifying information expected to be processed within each application and information system. From the business goals and business processes supported by the information systems, the level of dependency of these systems is determined and the possible losses as a result of disruptions assessed. Establishment of the maximum permissible loss subsequently leads to formulating the required demands of availability, integrity and confidentiality. That will lead, based on this, to choosing sufficient additional measures.

In order to provide more appropriate levels of protection to the information assets entrusted to Unit4, data must be classified according to the risks associated with its storage, processing and transmission within the realms of Unit4. Consistent use of the data classification policy will facilitate more efficient business activities and lower the costs of ensuring adequate information security. The data classification policy is an addition of the Information Security Policy.

Classification availability

Class	Security requirement
High	If the information is not available, Unit4 Global SaaS Ops will suffer great losses.
Medium	If the information is not available, Unit4 Global SaaS Ops will suffer, at most, slight losses.
Low	If the information is not available, Unit4 Global SaaS Ops will suffer no losses.

Classification integrity

Class	Security requirement
High	If the information is incorrect, incomplete or untimely, Unit4 Global SaaS Ops will suffer great losses. Incorrect data, such as in management information, will lead to inferior management. Occasional inaccuracies/incompleteness in the data are acceptable.
Medium	Incorrect, incomplete or untimely information will lead to slight losses. Limited

	absolute and lower requirements of the accuracy/completeness of the data.
Low	Incorrect, incomplete or untimely information will not lead to losses. No requirements of the accuracy/completeness of the data.

Classification confidentiality

Class	Security requirement
High	Information intended for internal use by Unit4 Global SaaS Ops. Inspection of this information by unauthorized people will bring very serious financial and/or public losses to the organization.
Medium	Information intended for internal use by Unit4 Global SaaS Ops Inspection of this information by unauthorized people will bring serious financial and/or public losses to the organization as a whole.
Low	Information intended for internal use by Unit4 Global Cloud Services. Inspection of this information by unauthorized people will bring possible financial and/or public losses to (parts of) the organization.

Information exchange with third parties

The Information Security Policy of Unit4 Global SaaS Ops focuses, in the first instance, on its own internal business processes. However, the exchange of information with external relations, for example through the Internet, is rapidly increasing. External relations could be Customers (business/private), supplier(s) of IT services and supervisory authorities. The aforementioned means that in Unit4 Global SaaS Ops security policy, the necessary attention is also paid to this form of data exchange. Information security does not limit itself anymore to just its own organization, but extends (increasingly) across the boundaries of its own organization.

Information destruction

Information stored on media including hard drives and tapes should be destroyed in a safe manner if they are defective, information is no longer needed or the retention of the information passed. All media sanitization processes are NIST 800-88 compliant.

Handling incidents

If Unit4 becomes aware of any unlawful access to their Services, or unauthorized access to these services, or unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a 'security incident'), Unit4 will promptly:

1. notify Customer of the Security Incident;
2. investigate the Security Incident and provide Customer with detailed information about the Security Incident; and
3. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

In order to be able to react appropriately to security incidents that may occur, these incidents will be classified. After a security incident is resolved, an evaluation takes place, and possible measures will be taken to prevent comparable incidents in the future or to limit the consequences of an incident.

Classification

Within Unit4 Global SaaS Ops, the following classes of security incidents are distinguished:

Class	Description
High	Directly threatening for the survival of Unit4 Global SaaS Ops. For example, an airplane crashing down onto the data center that Unit4 Global SaaS Ops uses.
Medium	Threatening for one or more primary business processes and in the long run even the survival of Unit4 Global SaaS Ops. For example, a disruption of customer processes or confidential information becoming public.
Low	In the long run threatening for the execution of the business processes.

Reporting and notifying

Users who notice a (suspicion of an) incident or violation of the information security will report this to the Information Security Officer. He/She will take care of classifying the incident and of further settlement. Depending on the classification, the Information Security Officer will notify management and the applicable Business Unit's.

Approach information security

1. Information security is a continual process.

   A reliable information provision demands continual attention. Alterations in the organization and/or the information provision, and the way in which the information provision is deployed for the purpose of operational management and process control, directly affect the reliability requirements demanded of the information provision and the measures that should be taken to ensure that.

2. Drawing up and implementing Information Security Policy.

   In this step, the objectives, preconditions and key points are recorded as well as the way in which the policy is translated into concrete measures. The policy is drawn up by the Information Security Officer.

3. Formulating and implementing basic security.

   The basis for information security is shaped by the Unit4 Global SaaS Ops standards framework, based on the Code of Practice for Information Security. This standards framework is a supplement of the Information Security Policy. The standards framework is subsequently translated into suitable security measures by the various sections of the organization. The establishment and prioritizing of the measures to be taken takes place based on risk analysis.

4. Additional security.

   There are systems that demand higher reliability requirements (in terms of Availability, Integrity and Confidentiality). The process of considering additional measures should be clear and reproducible. The additional measures are subsequently implemented and communicated.

5. Security management and review

Information security requires a continual effort (security management) and is therefore not a one-off activity. Reliable information provision demands constant attention. Following implementation, it is checked that the measures are indeed executed as intended (review). Periodic evaluation is necessary to determine if the chosen measures still suffice and will be adjusted where necessary.

Under responsibility of the Information Security Officer, within the various business units, checks will be carried out on:

- The presence of adequate security plans.
- The compliance with the specified standards and the implementation of the necessary additional security measures.
- The involvement and care of management for the lasting effect of the measures.

In addition, investigations are carried out in the internal audits into the various aspects in relation to information security.

The shortcomings, identified during the review, will be signaled and advice will be given regarding the measures to be taken in order to eliminate the faults.

Organization of the information security staff

Collaboration and coordination

At policy level and at executive level, collaboration and coordination takes place with regard to the activities to be carried out; approach, measures, awareness, reporting of incidents and arrangement of the security organization.

Within the context of the collaboration and coordination, functional consultation with the line managers exists under chairmanship of the Information Security Officer. Specialists from other disciplines can also be requested to participate in this consultation, such as, for example, support department employees.

Job specification of roles and responsibilities

A description of the roles, tasks and responsibilities should be part of the job description of the employee concerned. The security philosophy of Unit4 Global SaaS Ops expects a duty of care and alertness from each employee. It is expected that everyone will act in agreement with the specified regulations, for example with regard to the use of passwords. Management is expected to encourage this conduct.

Management

Management is ultimately responsible for the policy and the arrangement of information security.

Line Management

Line Management is primarily responsible for choosing, executing and upholding the information security measures. Line Management should hereby act in agreement with the specified Information Security Policy and the related regulations.

Line Management is, within their area of responsibility, among other things, responsible for:

- Allocating adequate resources for managing the information security.
- Allocating ownership to information and information systems.
- Ensuring adequate knowledge and awareness with regard to information security among employees and contract employees.

- Guaranteeing that the roles, tasks and responsibilities are recorded in the job descriptions of the employees and contracts with third parties.
- Periodic monitoring as to whether employees and contract employees comply with the Information Security Policy and related regulations and procedures.
- Taking necessary security-related measures following alterations of tasks and responsibilities of employees, suspension or termination of employment, termination of assignments or contracts.
- Communicating, within their own area of responsibility, the necessity of information security and the applicable policy regulations (awareness).
- Offering support with the implementation of the organization-wide common reliability standards and security measures and monitoring this.
- Establishing operational guidelines and procedures in relation to information security (tactical/operational).

Information Security Officer

The Information Security Officer is in charge of the general management of the execution of the Information Security Policy of Unit4 Global SaaS Ops and is responsible for formulating, maintaining and publicizing the Information Security Policy and related regulations. In addition, the Information Security Officer is responsible for:

- Initiating the establishment, evaluation and adjustment of the policy for information security (strategic/tactical).
- Coordinating the risk assessment and risk management processes.
- Development of the information security organization.
- Giving advice on promoting the security awareness of employees.
- Initiating information security measures and projects.
- Guiding the implementation of information security measures.
- Checking implemented information security measures.
- Reporting progress and bottlenecks upon the introduction of information security measures.
- Reviewing the status of the information security within Unit4 Global Cloud Ops and monitoring the security risks Unit4 Global SaaS Ops as a whole is running.
- Collating and reporting about information security incidents.
- Reporting, invited and uninvited, about the status and findings of the information security within the organization.
- Remaining aware of the developments in relation to information security both within and outside Unit4 Global SaaS Ops.
- Advising Line Management with regard to translating the Information Security Policy into information security plans for their areas of responsibility and with regard to the implementation of these plans.
- Advising Line Management concerning the making of agreements when exchanging data with other sections of the organization and with third parties.
- Evaluating, selecting and proposing applicable products, methodologies or working methods with regard to the information security.
- Keeping up with the developments in relation to information security.

Internal audits

Internal auditors test, on behalf of management and in consultation with the Information Security Officer, whether the responsible line management of the business units realizes the policy and complies with the security standards. Reports of the internal audits go to management.

Legal assurance

Legal assurance fulfils a stipulating role in the legal domain. Legal assurance translates legislation into legal frameworks and informs the business units about this. This applies also to legislation in relation to information provision and privacy.

Unit4 Global SaaS Ops employees

All employees are responsible for the security of information and information systems within their area of responsibility, in line with the Information Security Policy and the related regulations, procedures and instructions. The responsibility includes:

- Abide by the Ten Golden Rules of information security.
- Handling information with care.
- Protecting resources against threats, such as, for example, loss, destruction, damage or unauthorized access.
- Reporting security incidents immediately.

Contract employees

Contract employees have the same responsibilities with regard to information security as Unit4 Global SaaS Ops employees.

Contract employees should deal confidentially with the information of Unit4 Global SaaS Ops, including following conclusion of the assignment. Following conclusion of the assignment, they are not allowed to be in the possession of any information from Unit4 Global SaaS Services. Use of information and access to systems is only permitted for the collaboration with Unit4 Global SaaS Ops and in the interest of Unit4 Global SaaS Services.

Ten golden rules for information security

1. Passwords are strictly personal.

Your passwords are strictly personal and should be used exclusively by you in order to gain access to the systems concerned. Therefore, do not give your passwords to third parties or to a colleague and store them in a safe place, so not in your diary or on a yellow sticky note!

2. Reporting security incidents.

The Professional Services Manager is the Security Officer within Unit4. It is important to report all security incidents to this person as soon as possible. Examples of incidents are a virus alert, a break-in or attempted break-in, or a door that should have been locked.

3. Duty of confidentiality.

Within Unit4, Customers' information is frequently used. Keep to the guidelines as to how to deal with this.

4. Code of conduct Internet and email use.

Take care when using internet and email, avoid unsafe sites and do not open emails from unknown people.

5. Familiarizing yourself with the Information Security Policy.

Within Outsourcing, the Information Security Policy and accompanying guidelines are applicable. Familiarize yourself with these via your manager.

6. Providing information to third parties via the telephone.

The key point is that requests for information by telephone about our Customers will never be granted. That also means that no information about Customers will be provided by telephone to people or organizations who claim to phone on behalf of those involved.

7. Clean desk / clear screen policy.

Confidential treatment of Customers' information includes, among other things, that each workplace is arranged in such a way that unauthorized people cannot access this information in your absence. That means that you should consciously lock your work station using the screen lock function whenever you leave your workplace. Neither is confidential information, such as files or reports, allowed to remain on your desk unattended or in a non-lockable cupboard. The printer is also a workplace; therefore remove Customers' information from the printer immediately following printing.

8. No confidential information in the waste bin.

The correct treatment of confidential information – including Customers' information – is very important within Unit4.

Destroying this information should also take place in a safe way. Therefore, paper shredders or paper containers are available. Use these, and never put confidential information in the waste bin or in a container in your room destined for waste paper.

9. Approaching unknown people.

Have you already been in the situation, that you encountered an unknown person in the room secured with security pass cards? Approach this person, introduce yourself and ask their reason for being in here. New colleagues, temporary employees or other hired staff appreciate being approached and in this way be able to make new contacts. However, people unauthorized to be in this space will be alerted to their infringement. Accompany these people to the person they wish to visit, or accompany them to the public part of the building.

10. Haste, stress, work pressure vs. information security.

Information security does not come free – it costs energy and often works against you whenever you are in a hurry and when the work pressure is high. However, information security is extremely important for your work and is part of the professional and competent completion of the work. Therefore, take it very seriously – Customers of Unit4 rely on this.