INFORMED 365

Information Security Management Policy

Information management is an essential part of good IT governance, which in turn is a cornerstone in corporate governance. An integral part of the IT governance is information security, in particular pertaining to personal information.

The core principles for Informed 365's information security management are aligned with ISO/IEC 27002, i.e.:

- Risk assessment
- Organising information security
- Asset management
- Human resources security
- Physical security
- Communications and operations management
- Access control
- System development and maintenance
- Information security incident management
- Business continuity management
- Compliance

In addition, we comply with OWASP's top 10 application security risks.

Information Security Policy

Security Goals
Informed 365 is committed to safeguard the confidentiality, integrity and availability of all physical and electronic information assets of the company to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security at Informed 365 are the following:

- Ensure compliance with all current laws, regulations and guidelines.
- Comply with requirements for confidentiality, integrity and availability.
- Establish controls for protecting Informed 365's data, source code and applications against theft, abuse and other forms of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimise the risk of security incidents.
- Ensure that Informed 365 is capable of continuing their services even if major security incidents occur.
- Ensure the protection of personal data (privacy).
- Ensure the availability and reliability of the services supplied and operated by Informed 365.
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001.
- Ensure that external service providers comply with Informed 365's information security needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems by clients and users.

Security Strategy
Informed 365's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the information security policy (this document).
It has been decided that information security is to be ensured by the policy for information security and a set of underlying and supplemental documents. In order to secure operations at Informed 365 even after serious incidents, Informed 365 shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.

The term information security is related to the following basic concepts:

- **Confidentiality:**
  The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Integrity:**
  The property of safeguarding the accuracy and completeness of assets.
- **Availability:**
  The property of being accessible and usable upon demand by an authorised entity.

Roles and Areas of Responsibility
The administration has the overall responsibility for managing Informed 365's values in an effective and satisfactory manner according to current laws, requirements and contracts.
The Chief Executive Officer, Chief Information Officer and the Executive Team have the overall responsibility for information security at Informed 365, including information security regarding personnel and IT security.

Owner of the Security Policy
The Chief Executive Officer and the Executive Team are the owners of the security policy (this document). Chief Executive Officer, Chief Information Officer and the Executive Team delegate the responsibility for security-related documentation to the CIO. All policy changes must be approved and signed by the Chief Executive Officer and Executive Team.

Chief Information Officer (CIO)
The Chief Information Officer (CIO) holds the primary responsibility for ensuring the information security.

System Owner
The system owner, in consultation with the IT department, is responsible for purchasing requirements, development and maintenance of information and related information systems. All systems and all types of information must have a defined owner. The system owner must define which users or user groups are allowed access to the information and what authorised use of this information consists of.

System Administrator
System administrators are persons administrating Informed 365's information systems and the information entrusted to Informed 365 by other parties. Each type of information and system may have one or more dedicated system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is retained.

Users
Employees are responsible for getting acquainted and complying with Informed 365's IT regulations. Questions regarding the administration of various types of information should be posed to the system owner of the relevant information, or to the system administrator.

Principles for Information Security

Risk Management:

Risk Assessment and Management

Informed 365's approach to security is based on risk assessments. It continuously assesses the risk and evaluates the need for protective measures. An overall risk assessment of the information systems is performed annually. Risk assessments identify, quantify and prioritise the risks according to relevant criteria for acceptable risks. Risk management is to be carried out according to criteria approved by the management at Informed 365.
All risk assessments must be approved by the management at Informed 365 and/or the system owners. If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.

Information Security Policy

The Chief Executive Officer and Executive Team shall ensure that the information security policy, as well as guidelines and standards, are utilised and acted upon. The Chief Executive Officer and Executive Team must ensure the availability of sufficient training and information material for all users, in order to enable the users to protect Informed 365's data and information systems. The security policy shall be reviewed and updated annually or when necessary, in accordance with principles described in ISO/IEC 27001. All important changes to Informed 365's activities, and other external changes related to the threat level, should result in a revision of the policy and the guidelines relevant to the information security.

Security Organisation in Informed 365

The Chief Executive Officer and Executive Team are primarily responsible for all security related matters. The security authority at Informed 365, including information security and IT security, has been delegated to the CIO. The CIO has executive responsibility for information security in connection with IT systems, information security and infrastructure. Informed 365's information security will be revised on a regular basis, through internal control and at need, with assistance from an external IT auditor.

The Chief Executive Officer and Executive Team have the following responsibilities:

- Review and recommend information security policy and accompanying documentation and general distribution of responsibility.
- Monitor substantial changes of threats against the information assets of the organization.
- Review and monitor reported security incidents.
- Authorise initiatives to strengthen information security.

Classification and control of assets

"Assets" include information assets such as software, code, algorithms and Informed 365’s applications and to a physical assets such as laptops, desktops, etc. Information and infrastructure are classified according to security level and access control. Informed 365 regularly carries out risk analyses in order to classify information based on how critical it is for operations (criticality). Users administrating information on behalf of Informed 365 are required to treat said information according to classification.

Information Security in Connection With Users of Informed 365's Services

Prior to Employment

Security responsibility and roles for employees and contractors are in place. A background check is carried out of all appointees to positions according to relevant laws and regulations. A confidentiality agreement is signed by employees, contractors or others who may gain access to sensitive and/or internal information.

During Employment

The IT regulations refer to Informed 365's information security requirements and the users' responsibility for complying with these regulations. The IT regulations should be reviewed regularly with all users and with all new hires. All employees and third-party users should receive adequate training and updating regarding the

Information security policy and procedures. Breaches of the Information security policy and accompanying guidelines will normally result in sanctions. Use of Informed 365's IT infrastructure for personal commercial activities is under no circumstances permitted.

Termination or Change of Employment
The responsibility for termination or change of employment is defined in a separate policy. Informed 365's assets are to be handed in at the conclusion of the need for the use of these assets.
Informed 365 changes / terminates access rights at termination or change of employment.

Securing Equipment and Data
Sensitive IT equipment and data must be protected against environmental threats (fires, flooding, temperature variations, etc.). Classification of equipment is based on risk assessments. Information classified as "sensitive" must not be stored on portable computer equipment (e.g. laptops). If it is necessary to store this information on portable equipment, the information must be password protected and encrypted in compliance with guidelines from the IT department. During travel, portable computer equipment should be treated as carry-on luggage.

IT Communications and Operations Management
The IT department ensures documentation of the IT systems according to Informed 365's standards. Changes in IT systems are only implemented if well-founded from a business and security standpoint. The IT department has emergency procedures in order to minimise the effect of unsuccessful changes to the IT systems. Operational procedures are documented. Documentation must be updated following all substantial changes.
Development, testing and maintenance is separated from operations in order to reduce the risk of unauthorised access or changes, and in order to reduce the risk of error conditions.

System Planning and Acceptance
Requirements for information security are taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes. Routines have been developed for change management and system development/maintenance. IT systems are dimensioned according to capacity requirements. The load is monitored in order to apply upgrades and adjustments in a timely manner. This is especially important for business-critical systems.

Protection against Malicious Code
Computer equipment must be safeguarded against virus and other malicious code. This is the responsibility of the CIO.

Back-Up
The IT department is responsible for carrying out regular backups and restore of these backups, as well as data storage on Informed 365's IT systems. Backups are stored externally or in a separate, suitably protected zone.

Use of Encryption
Storage and transfer of sensitive information should be encrypted or otherwise protected.

Monitoring of System Access and Usage
Access and use of IT systems is logged and monitored in order to detect unauthorised information processing activities. Usage is traceable to a specific entity, e.g. a person or a specific system. The IT department registers substantial disruptions and irregularities of system operations, along with potential causes of the errors. Capacity, uptime and quality of the IT systems are monitored in order to ensure reliable operation and availability. The IT department logs security incidents for all essential systems.

Access Control
Business requirements: Written guidelines for access control and passwords based on business and security requirements are in place. Guidelines are re-evaluated on a regular basis. Guidelines contain password requirements (frequency of change, minimum length, character types which may/must be utilised, etc.) and regulate password storage.

User Administration and Responsibility
Users accessing systems must be authenticated according to guidelines. Users have unique combinations of usernames and passwords. Users are responsible for any usage of their usernames and passwords. Users should keep their passwords confidential and not disclose them unless explicitly authorised by the CIO.

Access Control / Authorization
Access to information systems is authorised by immediate superiors in accordance with the system owner directives. This includes access rights, including accompanying privileges. Authorisations should only be granted on a "need to know" basis and regulated according to role.

Mobile Equipment and Remote Workplaces
Remote access to Informed 365's computer equipment and services is only permitted if the security policy has been read and understood and the IT regulations signed.
Remote access to Informed 365's systems may only take place through security solutions approved by the IT department.

Security of System Files
All changes to production environments should comply with existing routines. The implementation of changes to the production environment should be controlled by formal procedures for change management, in order to minimise the risk of damaged information or information systems.

Security in Development and Maintenance
Systems developed by Informed 365 must satisfy definite security requirements, including data verification, securing the code before being put in production, and use of encryption where required.
All software should be thoroughly tested and formally accepted by the system owner and the IT department before being transferred to the production environment.

Responsibility for Reporting
All breaches of security, along with the use of information systems contrary to routines, should be treated as incidents. All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to management or directly to the CIO.

Measurements
Routines have been developed for incident management and reporting. The routines should contain measures for preventing repetition as well as measures for minimising the damage.

Collection of evidence
The IT security manager should be familiar with simple routines for collecting evidence.

Continuity Planning
A plan for continuity and contingencies covering critical and essential information systems and infrastructure should exist. The continuity plan(s) should be based on risk assessments focusing on operational risks. The continuity plan(s) should be consistent with Informed 365's overall contingencies and plans. The continuity plan(s) should be tested on a regular basis to ensure adequacy, and to ensure that management and employees understand the implementation.

Compliance With OWASP Top 10 Web Application Security Risks

1. **Injection**. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2. **Broken Authentication**. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities temporarily or permanently.

3. **Sensitive Data Exposure**. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. **XML External Entities (XXE)**. Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5. **Broken Access Control**. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
6. **Security Misconfiguration**. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
7. **Cross-Site Scripting XSS**. XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
8. **Insecure Deserialization**. Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
9. **Using Components with Known Vulnerabilities**. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
10. **Insufficient Logging & Monitoring**. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.