Corporate Information Security Policy

Version v1.0
February 15, 2017

Table of Contents

1 Document Control
1.1 Revision History
2 Introduction
2.1 Information Security Mission Statement
2.2 Philosophy of Protection
2.3 Scope
2.4 Definition of Information Security
2.5 Terms and Definitions
2.6 Information Security Policy Structure
3 Risk Assessment Policy
3.1 Purpose
3.2 Scope
3.3 Policy Statements
3.3.1 Responsibilities
3.3.2 Policy
3.4 Risk Assessment
3.4.1 Establish Context
3.4.2 Identify Risks
3.4.3 Analyze Risks
3.4.4 Evaluate Risks
3.5 Risk Treatment
3.6 Communication and Monitoring
4 Information Security Policies
4.1 Management Direction for Information Security
4.1.1 Policies for Information Security
4.1.2 Review of the Policies for Information Security
5 Organization of Information Security
5.1 Internal Organization
5.1.1 Information Security Roles and Responsibilities
5.1.2 Segregation of Duties
5.1.3 Contact with Authorities
5.1.4 Contact with Special Groups
5.2 Mobile Devices and Teleworking
5.2.1 Mobile Device Policy
5.2.2 Teleworking
6 Human Resources Security
6.1 Prior to Employment
6.1.1 Screening
6.1.2 Terms and Conditions of Employment

6.2 During Employment
6.2.1 Management Responsibilities
6.2.2 Information Security Awareness, Education and Training
6.2.3 Disciplinary Process
6.3 Termination and Change of Employment
6.3.1 Termination or Change of Employment Responsibilities

7 Asset Management
7.1 Responsibility for Assets
7.1.1 Inventory of Assets
7.1.2 Ownership of Assets
7.1.3 Acceptable Use of Assets
7.1.4 Return of Assets
7.2 Information classification
7.2.1 Classification of Information
7.2.2 Labeling of Information
7.2.3 Handling of Assets
7.3 Media Handling
7.3.1 Disposal of media

8 Access Control
8.1 Business Requirements of Access Control
8.1.1 Access Control Policy
8.1.2 Access to Networks and Network Services
8.2 User Access Management
8.2.1 User Registration and De-registration
8.2.2 User Access Provisioning
8.2.3 Management of Privileged Access Rights
8.2.4 Management of Secret Authentication Information of Users
8.2.5 Review of User Access Rights
8.2.6 Removal or Adjustment of Access Rights
8.3 User Responsibilities
8.3.1 Use of Secret Authentication Information
8.4 System and Application Access Control
8.4.1 Information Access Restriction
8.4.2 Secure Log-on Procedures
8.4.3 Password Management System
8.4.4 Use of Privileged Utility Programs
8.4.5 Access Control to Program Source Code

9 Cryptographic Controls
9.1.1 Policy on the Use of Cryptographic Controls
9.1.2 Key Management

10 Physical and Environmental Security
10.1 Secure Areas
10.1.1 Physical Security Perimeter

10.1.2 Physical Entry Controls
10.1.3 Securing Offices, Rooms and Facilities
10.1.4 Protecting Against External and Environmental Threats
10.2 Equipment
10.2.1 Equipment Siting and Protection
10.2.2 Supporting Utilities
10.2.3 Cabling Security
10.2.4 Equipment Maintenance
10.2.5 Unattended User Equipment
10.2.6 Clear Desk and Clear Screen Policy

11 Operations Security
11.1 Operational Procedures and Responsibilities
11.1.1 Documented Operating Procedures
11.1.2 Change Management
11.1.3 Capacity Management
11.1.4 Separation of Development, Testing and Operational Environments
11.2 Protection from Malware
11.2.1 Controls Against Malware
11.3 Backup
11.3.1 Information Backup
11.4 Logging and Monitoring
11.4.1 Event Logging
11.4.2 Protection of Log Information
11.4.3 Administrator and Operator Logs
11.4.4 Clock Synchronization
11.5 Control of Operational Software
11.5.1 Installation of Software on Operational Systems
11.6 Technical Vulnerability Management
11.6.1 Management of Technical Vulnerabilities

12 Communications Security
12.1 Network Security Management
12.1.1 Network Controls
12.1.2 Security of Network Services
12.1.3 Segregation in Networks
12.2 Information Transfer
12.2.1 Information Transfer Policies and Procedures
12.2.2 Agreements on Information Transfer
12.2.3 Electronic Messaging
12.2.4 Confidentiality or Non-disclosure Agreements

13 System Acquisition, Development and Maintenance
13.1 Security Requirements of Information Systems
13.1.1 Information Security Requirements Analysis and Specification
13.1.2 Securing Application Services on Public Networks
13.1.3 Protecting Application Services Transactions

13.2 Security in Development and Support Processes
13.2.1 Secure Development Policy
13.2.2 System Change Control Procedures
13.2.3 Technical Review of Applications after Operating Platform Changes
13.2.4 Restrictions on Changes to Software Packages
13.2.5 Secure System Engineering Principles
13.2.6 Secure Development Environment
13.2.7 System Security Testing
13.2.8 System Acceptance Testing
13.3 Test Data
13.3.1 Protection of Test Data

14 Supplier Relationships
14.1 Information Security in Supplier Relationships
14.1.1 Information Security Policy for Supplier Relationships
14.1.2 Addressing Security within Supplier Agreements
14.1.3 Information and Communication Technology Supply Chain

15 Information Security Incident Management
15.1 Management of Information Security Incidents and Improvements
15.1.1 Responsibilities and Procedures
15.1.2 Reporting Information Security Events
15.1.3 Reporting Security Weaknesses
15.1.4 Assessment of and Decision on Information Security Events
15.1.5 Response to Information Security Incidents
15.1.6 Learning from Information Security Incidents
15.1.7 Collection of Evidence

16 Information Security Aspects of Business Continuity Management
16.1 Information Security Continuity
16.1.1 Planning Information Security Continuity
16.1.2 Implementing Information Security Continuity
16.2 Redundancies
16.2.1 Availability of Information Processing Facilities

17 Compliance
17.1 Compliance with Legal and Contractual Requirements
17.1.1 Identification of Applicable Legislation and Contractual Requirements
17.1.2 Intellectual Property Rights
17.1.3 Protection of Records
17.1.4 Privacy and Protection of Personally Identifiable Information
17.1.5 Regulation of Cryptographic Controls
17.2 Information Security Reviews
17.2.1 Independent Review of Information Security
17.2.2 Compliance With Security Policies and Standards
17.2.3 Technical Compliance Review

1 Document Control

The Reflektive document control process is followed for any document produced. The process accomplishes the following:

- Track document changes;
- Ensure that each document and any subsequent changes to the document have been reviewed and agreed upon by stakeholders; and
- Review and approval for information security management.

1.1 Revision History

Version	Date	Change Log	Approved By
1.0	2/15/2017	Initial Release	Jimmie Tyrrell

2 Introduction

2.1 Information Security Mission Statement

Reflektive and Reflektive employees have an inherent responsibility to protect the physical information assets of the company as well as confidential customer data and intellectual capital owned by the company. These critical assets must be safeguarded to mitigate any potential impacts to Reflektive and Reflektive's customers. Information security at Reflektive is, therefore, a critical business function that should be incorporated into all aspects of Reflektive's business practices and operations.

To achieve this objective, policies, procedures, and standards have been created to ensure secure business practices are in place at Reflektive. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

2.2 Philosophy of Protection

Reflektive's philosophy of protection provides the intent and direction behind our protection policies, procedures, and control. Our protection philosophy is comprised of three tenets:

1. **Security is everyone's responsibility**. Maintaining an effective and efficient security posture for Reflektive requires a proactive stance on security issues from everyone. Security is not "somebody else's problem"; as an employee or contractor of Reflektive you have the responsibility to adhere to the security policies and procedures of the company and to inform both Reflektive's security team and management of those who are not doing the same.
2. **Security permeates the Reflektive organization**. Security is not just focused on physical and technical "border control." Rather, Reflektive seeks to ensure reasonable and appropriate levels of security awareness and protection throughout our organization and infrastructure. There is no place in our business where security is not a consideration.
3. **Security is a business enabler**. A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace, and must be treated as a valued commodity.

The tenets of our philosophy of protection are mutually supportive; ignoring any one tenet in favor of another undermines the overall security posture of our organization.

2.3 Scope

This Information Security Policy outlines the framework for management of information security and applies to all people, resources, policies, practices and procedures under the purview of the Compliance Committee at Reflektive. The “Compliance Committee” refers to the group of Reflektive employees to whom the Chief Information Security Officer delegates security tasks.

2.4 Definition of Information Security

Information Security centers on the following three objectives for protecting information: **Confidentiality**, **Integrity**, and **Availability**. The policies in this document support these objectives.

2.5 Terms and Definitions

For the purpose of this document, the following terms and definitions apply.

- **Asset** – Anything that has value to the organization
- **Control** – Means of managing risk, including policies, procedures, guidelines and practices
- **Guideline** – A description that clarifies what should be done and how
- **Information Processing Facilities** – Any information processing system, service or infrastructure, or the physical locations housing them
- **Information Security** – Preservation of confidentiality, integrity and availability of information
- **Information Security Event** – Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
- **Information Security Incident** – A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
- **Information Security Management System** – Part of the overall management system, a set of policies and procedures based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
- **Information System** – Application, service, information technology asset, or any other information handling component
- **Policy** – Overall intention and direction as formally expressed by management
- **Procedure** – Guidance containing step-by-step instructions to implement various policies, standards, and guidelines
- **Process** – Set of interrelated or interacting activities which transforms inputs into outputs
- **Review** – Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
- **Risk** – Effect of uncertainty on objectives
- **Stakeholder** – Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

- **Standard** – Guidance consisting of specific low level mandatory controls to help enforce and support the information security policy
- **Threat** – Potential cause of an unwanted incident, which may result in harm to a system or the business
- **Verification** – Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
- **Vulnerability** – Weakness of an asset or control that can be exploited by one or more threats

2.6 Information Security Policy Structure

Reflektive's Information Security Policies are structured in such a way to give flexibility as required by business objectives and needs while maintaining a 'level playing field' across the company. Frequently, the weakest link is the link that breaks the security chain and causes a breach in security. Through consistent application of information security across the company, any weak areas are compensated for and the organization is stronger overall.

Information Security Policy follows this tiered structure:

- Information Security Mission Statement
- Information Security Policy
- Information Security Standards and Processes
- Information Security Specific Configurations and Procedures

The hierarchy lends support as you progress up the tiers and becomes more detailed as you progress down the tiers. In this way, all actions taken have a basis in policy and directly support the policy or policies they are governed by. To illustrate this hierarchy, descriptions of the various levels are given below.

Information Security Mission Statement – This is the overall management direction in regards to Information Security at Reflektive. It is broad in scope and sets the expectations for protecting the company's information resources. It is contained in this document.

Information Security Policy – This document is the Information Security Policy that implements the overall guidance of the Information Security Mission Statement. Policies are somewhat broad but topical in nature (centered on specific Information Security topics). Reflektive's Information Security Policy is organized in accordance with ISO 27002, an international standard and seeks compliance with other regulatory and compliance mandates where applicable. This policy applies equally to everyone within the company, regardless of location.

Information Security Standards and Processes – These are collections of standards and processes that are to be used to implement the given policy they reference. Standards may dictate a type of technology to use, but may stop before naming a particular product (depending on the policy and standard subject). Processes will detail the steps to take to fulfill the goals of a particular policy. Standards and Processes will be published under separate titles and may be regionalized to fit the conditions at different locations (i.e., there may be one set of standards for a particular policy in the United

States, and a different set in Germany). Standards and Process will clearly delineate where they apply.

Information Security Specific Configurations and Procedures – These are very specific details that support the implementation of the standards and processes given above. These will include specific products and configuration details, or step-by-step procedures to implement processes. These are very highly localized and will apply to the environment for which they were written (i.e., there may be a specific configuration for Oracle systems that is different from Windows configurations). These will be published under separate titles where directed.

3 Risk Assessment Policy

3.1 Purpose

To establish a framework to identify, assess and counter security risks faced by Reflektive's information and information systems assets.

3.2 Scope

The policy is applicable for:

- All Confidential Reflektive Information assets.
- Information belonging to Reflektive's business partners, end consumers and contracted 3rd parties.
- Infrastructure critical to the protection of confidentiality, integrity and availability of all Reflektive and related information assets.

3.3 Policy Statements

3.3.1 Responsibilities

- Chief Information Security Officer (CISO) is responsible for the implementation, maintenance and continual improvement of this policy.
- All asset owners are responsible for providing necessary information for the assets owned and managed by them for assisting CISO in risk management.
- Executive management is responsible for reviewing and approving the Risk Management Plan, which includes Risk Assessment and Treatment.

3.3.2 Policy

- Risk assessment shall be carried out annually or at instances of substantial changes to processes, infrastructure, people or technology.
- Risk assessments shall be conducted using industry best practices customization.

3.4 Risk Assessment

3.4.1 Establish Context

Reflektive should first consider why they are performing a risk assessment. Determine the external and internal contexts that drive the risk assessment. These considerations help

establish the risk acceptance criteria against which the risk analysis will be compared and evaluated. Risk acceptance criteria depend on contexts such as company policies, goals, objectives, stakeholder interests, laws and regulations.
In developing risk acceptance criteria consider the following:

- Business criteria
- Legal and regulatory aspects
- Operational considerations
- Technological aspects
- Financial considerations
- Social and humanitarian factors

3.4.2 Identify Risks

Once the context and risk criteria have been established, identify all assets in scope.
Maintain an asset inventory with a short description of each asset.
Identify all threats against the assets in scope.

3.4.3 Analyze Risks

Risk analysis involves estimating the level of the risks that had been identified against the asset inventory. The level of risk is calculated by estimating the likelihood of a threat and its impact on the business.

3.4.4 Evaluate Risks

Evaluate risks by comparing the risk analysis results with the risk acceptance criteria. The contexts that were established at the beginning of the assessment should guide whether or not risks are acceptable or tolerable.

3.5 Risk Treatment

There are four risk treatment options: 1) risk modification, 2) risk retention, 3) risk avoidance, and 4) risk sharing.

- **Risk modification** involves selecting and implementing controls to mitigate risk to an acceptable level.
- **Risk retention** is the acceptance of the burden of loss or benefit of gain from a particular risk. Certain risks may be accepted based on risk evaluation. However, some risks such as those that could result in non-compliance with laws and regulations may not be accepted.
- **Risk avoidance** involves withdrawing or discontinuing an activity that is vulnerable to risk. The negative costs of a certain activity may be deemed to outweigh its benefit.
- **Risk sharing** involves another party sharing the burden of loss or benefit of gain for a risk. For example, Reflektive can pay an insurance company to share the responsibility of damage from a threat event. The business impact of such an event and therefore the level of risk are reduced.

3.6 Communication and Monitoring

This entire risk assessment and risk treatment process must be documented and monitored, and will be reviewed annually to improve and update risk management at Reflektive.

4 Information Security Policies

4.1 Management Direction for Information Security

4.1.1 Policies for Information Security

Policy

Management must set direction and provide support for members of the Information Security Team at Reflektive to establish, issue and communicate information security policies through education, training and awareness.

Explanation

In order to effectively establish comprehensive information security policies, processes and practices that will support the business, and the company's mission and objectives, it is necessary to establish management direction on, and commitment to information security.

Standard

The CISO office will lead efforts to develop the corporate Information Security Policy using this procedure.

1. Review business requirements;
2. Establish an information security policy that meets the requirements for customer engagements;
3. Develop controls, policies, processes, and procedures to support confidentiality, integrity and availability of data in a manner that supports business and operational needs;
4. Create a draft of the information security policy for key stakeholder review by key stakeholders representing the IT department and other parties with a vested interest in security policies; and
5. Obtain approval from key stakeholders for the security policy.

Authorities

ISO 27001 A.5.1.1; SOC 2: CC1.2, CC2.3, CC3.2

4.1.2 Review of the Policies for Information Security

Policy

The information security policy must be reviewed on an annual basis and updated when required.

Explanation

To ensure information security policies remain current with evolving business needs and technological changes.

Standard

The procedure to timely review and update the Information Security Policy is as follows:

1. On an annual basis, the CISO shall conduct a comprehensive review of information security policies;
2. Update the information security policy as required to meet security, business, and compliance objectives;
3. Create an updated draft of the information security policy for key stakeholder review by the Compliance Committee and other parties with a vested interest in security policies; and
4. Obtain approval from key stakeholders for the updated security policy.

Authorities

ISO 27001 A.5.1.2; SOC 2: CC1.2, CC2.2, CC2.3, CC3.2

5 Organization of Information Security

5.1 Internal Organization

To establish a management framework to initiate and control the implementation and operation of information security within the organization.

5.1.1 Information Security Roles and Responsibilities

Policy

Implementation of information security activities across Reflektive must be coordinated and managed by the CISO. The CISO must take overall responsibility for information security that has been delegated.

Explanation

To ensure that information security activities are carried out and resolved in a timely manner.

Standard

The CISO must establish an information security program to manage and coordinate information security activities across the company by:

- Providing leadership on methodologies and processes for information security;
- Promoting information security education, training and awareness throughout the company;
- Identifying significant threat changes and exposures to threats of assets associated with information security;
- Ensuring the Incident Management Process is followed for all suspected or actual information incidents;
- Evaluating information received during and after an information security incident;
- Implementing performance measurement processes for security controls;
- Ensuring information security activities are in compliance with the Information Security Policy;
- Identifying responses to remediate activities that are not in compliance with policies, standards or best practices;
- Coordinating the implementation of information security controls; and
- Recommending appropriate actions in response to identified information security incidents and initiating audits where necessary.

<u>Security Coordination Across Departments</u>

A cross-functional information security working group shall be established to:

- Develop and implement information security policies, standards and guidelines;
- Promoting the consistent application of information security programs; and
- Identify issues related to information security disciplines and critical information asset protection

Each asset will have an “owner”, who may delegate responsibilities, but remains ultimately responsible for the asset(s).

<u>Security Coordination Between Customers and Partners</u>

To meet security requirements that exist between customers and partners, it will be necessary from time to time to coordinate security efforts with these entities. This ensures that services are provided in a manner that is highly available and secure.

Authorities

ISO 27001 A.6.1.1; SOC 2: CC1.2

5.1.2 Segregation of Duties

Policy

A single person must not be able to access, modify or use assets without authorization or detection. The person responsible for initiating an event must be separate from the

person authorizing an event, otherwise the person must be monitored and provide an audit trail.

Explanation

To reduce risk of loss, fraud, error and unauthorized changes to information.

Standard

Assign an event initiator separate from the event authorizer. If this is not possible, monitor the event and require audit trails. Consider the possibility of collusion in designing controls and mitigate opportunities for any one individual to conceal errors or irregularities by limiting access rights to a single user.

Authorities

ISO 27001 A.6.1.2; SOC 2: CC5.2, CC5.4

5.1.3 Contact with Authorities

Policy

Appropriate contacts shall be maintained with local law enforcement authorities, emergency support staff and service providers.

Explanation

To facilitate timely response from and coordination with outside authorities during information security incidents or investigations.

Standard

All contact and cooperation with third parties on security matters will be coordinated through the CISO or a designated appointee of the CISO.

Authorities

ISO 27001 A.6.1.3; SOC 2: CC2.5, CC6.2

5.1.4 Contact with Special Groups

Policy

Appropriate contacts shall be maintained with specialist security forums and professional associations.

Explanation

To promote and further employee knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities.

Standard

Have appropriate personnel subscribe to alerts from United States Computer Emergency Readiness Team (US-CERT) and National Institute of Standards and Technology (NIST) to receive timely information about security topics and threats.

Authorities

ISO 27001 A.6.1.4; SOC 2: CC1.3, CC1.4

5.2 Mobile Devices and Teleworking

5.2.1 Mobile Device Policy

Policy

Appropriate controls must be implemented to mitigate security risks associated with the use of mobile devices.

Explanation

To protect information stored on mobile devices from loss or unauthorized access.

Standard

Register company mobile devices to the specified user with an agreement including:

- Restriction of software installation
- Restriction of connection to information services
- Use of secure access controls
- Use of malware protection
- Enable remote disabling, erasure or lockout
- Use of VPN or SSL to encrypt communication

Privately owned mobile devices used for business require agreements similar to the above.

Authorities

ISO 27001 A.6.2.1; SOC 2: CC5.6

5.2.2 Teleworking

Policy

Teleworking must employ security controls to ensure that information resources are not compromised.

Explanation

To protect information accessed through teleworking arrangements from loss or unauthorized access.

Standard

Control includes:

- Persons who will be doing part or all of their work off Reflektive's premises (teleworking) must be authorized to do so by an appropriate authority within the organization;
- All teleworking agreements must include appropriate measures, based on a risk assessment, to protect the security of information assets; and
- Teleworkers must follow the agreed security procedures at all times unless specifically authorized.

For purposes of this standard, Reflektive may include all telework requirements and procedures in its Employee Handbook in lieu of a separate teleworking agreement.

Authorities

ISO 27001 A.6.2.2; SOC 2: CC5.6

6 Human Resources Security

6.1 Prior to Employment

To ensure that employees and contractors understand their responsibilities, and are suitable for the roles for which they are considered.

6.1.1 Screening

Policy

Personnel must be screened prior to entering a working relationship with Reflektive.

Explanation

To assure that information assets are protected from personnel that may not be trustworthy of the responsibilities associated with security protection and to ensure that personnel are qualified for their respective positions.

Standard

Human Resources must conduct background checks prior to hiring personnel. Upon legal consent from prospective candidates, checks that are legally permitted and relevant to the prospective position may include:

- Criminal check
- Credit check
- Employment verification
- Education verification
- Identity verification

Information gathered during the investigation must inform the hiring decision.

Authorities

ISO 27001 A.7.1.1; SOC 2: CC1.3, CC1.4

6.1.2 Terms and Conditions of Employment

Policy

The terms and conditions of employment must document the responsibility of personnel for information and information systems security.

Explanation

To make clear to all employees their responsibilities for maintaining and promoting security within the organization during and subsequent to their employments as well as the sanctions for not doing so.

Standard

Personnel must agree to their responsibility for information security in the terms and conditions of employment. The terms and conditions reflect the security policy in addition to clarifying:

- That all users who are given access to sensitive information will sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;
- The employee's, contractor's, or third party's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation;
- Responsibilities for the classification of information and management of company assets associated with information systems and services handled by the employee;
- Responsibilities of the user for the handling of information received from other companies or external parties;
- Responsibilities of the company for handling of personal information, including personal information created as a result of, or in the course of, employment with the company;
- Responsibilities that are extended outside Reflektive premises and outside normal working hours; and
- Actions to be taken if the user disregards Reflektive security requirements.

Authorities

ISO 27001 A.7.1.2; SOC 2: CC3.2, C1.3

6.2 During Employment

To ensure that all employees, and contractors are aware of and fulfill their information security responsibilities.

6.2.1 Management Responsibilities

Policy

Management must ensure personnel comply with security policies and procedures.

Explanation

To establish management responsibilities for ongoing support and implementation of information security.

Standard

The CISO must delegate security compliance to managers of each group. Managers must understand, make known and ensure security responsibilities for their employees, contractors and third party users in accordance with Reflektive established policies.

Authorities

ISO 27001 A.7.2.1; SOC 2: CC1.2

6.2.2 Information Security Awareness, Education and Training

Policy

Personnel must receive appropriate information security training and be informed of changes to information security policy and practices.

Explanation

To increase personnel awareness and understanding of security threats, risks and concerns and information security policies and procedures.

Standard

Reflektive shall provide basic security awareness training to all information system users (including department, agency and board directors, heads and chairs, and contractors) as part of initial training for new users, and as required by system changes. All employees have responsibility for some degree of physical security, information security and information technology security, so all employees and third party contractors are required to complete this basic security awareness training upon initial employment and maintain that training annually.

<u>Security Awareness Program</u>

Key components of security education include information concerning the prevention and identification of possible security breaches and the process for informing the security administration team. Incident identification and response education must follow requirements outlined in the Information Security Incident Management Policy.

Training Acknowledgment

Upon completion of new employee and annual Security Awareness Training, individuals will acknowledge that s/he has completed and understands Reflektive security policies. Records of completed security awareness training will be maintained by Human Resources.

Ad Hoc Education

Human Resources and Management will engage employees and contractors with periodic reminders to cover both general security topics and specific issues of relevance. Appropriate efforts to raise and maintain awareness of security issues may include topic-specific emails, discussion in department or team meetings, and signage.

Authorities

ISO 27001 A.7.2.2; SOC 2: CC2.2, CC2.3, CC2.5, CC2.6, CC3.2

6.2.3 Disciplinary Process

Policy

Security breaches or policy violations caused by personnel must be reviewed by Management.

Explanation

To ensure a process is in place to review the activities of personnel who commit a security breach or policy violation.

Standard

In the instance of a security breach, the Operations team may conduct an investigation to identify the source of the breach. The Operations department will follow its Incident Response Plan, including standards for collection of evidence and chain of custody of evidence. Given reasonable evidence to determine fault, Chief Security Officer, Human Resources and Management will determine appropriate sanctions and user awareness.

The disciplinary process for employees who have committed a security breach begins with an investigation and verification of a security breach. Disciplinary actions shall be considered as constructive procedures for the purpose of correcting inappropriate work behavior that has or may lead to a security breach.

The progressive action to be taken by Management will follow established disciplinary process and may include discussion of the issue, verbal warning, written warning, suspension, or termination. Disciplinary actions will be administered in a uniform basis throughout the organization. However, each offense must be judged on a case-by-case basis with consideration given to the employee's past record.

Authorities

ISO 27001 A.7.2.3; SOC 2: CC6.2

6.3 Termination and Change of Employment

To protect the organization's interests as part of the process of changing or terminating employment.

6.3.1 Termination or Change of Employment Responsibilities

Policy

Responsibilities for employment termination must be documented and communicated to relevant parties.

Explanation

To ensure information security responsibilities upon termination of employment are defined, assigned and communicated.

Standard

Upon termination or change of employment notification from Human Resources, access to relevant Reflektive IT managed systems are disabled within twenty-four hours of the effective termination or change of employment date.

Accounts of terminated personnel with privileged access must be disabled immediately.

Authorities

ISO 27001 A.7.3.1; SOC 2: CC5.2, CC5.4

7 Asset Management

7.1 Responsibility for Assets

To identify organizational assets and define appropriate protection responsibilities.

7.1.1 Inventory of Assets

Policy

An inventory of all critical assets associated with information systems must be documented and maintained.

Explanation

To identify and manage information and information technology assets associated with information systems or services ("assets"), to provide control and accountability, support

strategic planning, enhance critical incident response, system planning, protection, maintenance and recovery.

Standard

Asset Management must regularly maintain a current inventory of major IT assets and apply an asset tag to IT hardware to keep track throughout its asset lifecycle.

Inventory must include:

- Type of asset;
- Asset identification number or tag;
- Assigned owner;
- Location (logical or physical location, range of physical locations if portable);
- Backup information (if appropriate);
- License information (if appropriate);
- Business value, security classification and level of protection; and
- Any additional data necessary to allow recovery from a disaster or otherwise assure continuity of operations.

Authorities

ISO 27001 A.8.1.1; SOC 2: CC3.1, A1.1, A1.2, A1.3

7.1.2 Ownership of Assets

Policy

Asset Owners and Asset Custodians must be designated for all assets associated with information systems.

Explanation

To designate custodians for assets with approved management responsibility for the protection of organizational assets associated with information and technology systems or services.

Standard

All software, hardware, and other devices that are signed out to an individual are the responsibility of the assigned individual to maintain and safeguard. The asset remains the property of Reflektive.

Responsibilities:

- Asset Owner – Information asset owners are responsible to classify assets, including data.
- Users – The individuals entrusted with the information assets are responsible for protecting the asset consistent with the security requirements defined by the custodians.

- Custodians – Information asset custodians are responsible for designing and implementing controls for protection of information on behalf of asset owner. These controls shall safeguard the confidentiality, integrity and availability of assets. Custodian shall also update asset inventory and ensure access is removed from those who no longer have a business need for the asset.
- Managers – Management shall take appropriate action to ensure that all users are aware of the actions pertaining to safeguarding assets in the organization.
- Application Development and Database Administrators – Administrators are responsible for implementing and monitoring approved access control solutions to ensure that all sensitive applications have the appropriate audit functions. The administrators may also be referred to as custodians.
- CISO – The CISO shall ensure that continuity of access control solutions meets the needs of asset owners to safeguard sensitive assets. The CISO shall also assess and monitor safeguards to ensure their compliance and report situations of non-compliance.

Authorities

ISO 27001 A.8.1.2; SOC 2: CC3.1, CC5.1

7.1.3 Acceptable Use of Assets

Policy

Rules for the acceptable use of information systems must be identified, documented and implemented.

Explanation

To prevent misuse or compromise of Reflektive information systems.

Standard

The CISO must document, implement and circulate the Acceptable Use Policy in the Employee Handbook for information assets, systems and services. The guidelines and procedures in the Acceptable Use Policy apply to all employees, contractors and third parties. Use of the system must be conditional on acceptance of the Acceptable Use Policy. This requirement must be formally agreed upon and auditable.

Authorities

ISO 27001 A.8.1.3; SOC 2: CC5.7, CC5.8

7.1.4 Return of Assets

Policy

Personnel must return Reflektive assets upon termination or change of employment.

Explanation

To ensure personnel return physical and information assets at termination of employment.

Standard

Human Resources must collect Reflektive assets from personnel before completing an exit interview. IT and Management will provide complete list of assets to Human Resources, who will review the list with user and collect assets.

Where the employee, contractor or third party uses personal equipment, secure erasure of software and data belonging to the organization must be completed.

Authorities

ISO 27001 A.8.1.4; SOC 2: CC5.6

7.2 Information classification

To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

7.2.1 Classification of Information

Policy

Reflektive information security classification system must take into account the legal, value, sensitivity and intended use of the information for IT. Information that is classified confidential is:

- Any information that originates within Reflektive
- Any information, documents and materials that Reflektive receives from outside parties.

Explanation

To define the information security classification system characteristics for information and information systems for IT.

Standard

Confidentiality of assets shall also be classified as:

- **Confidential** – This classification applies to sensitive business information where unauthorized disclosure could cause serious impact and/or adversely affect Reflektive, its employees, member financial institutions, business partners and/or the brand. All customer, consumer and credit card information shall be classified as Confidential.
- **Internal** – This classification applies to all other non-public information that does not fit into Secret or Confidential classification. While its unauthorized disclosure is against procedure, it is not expected to result in serious or adverse consequences to

Reflektive, its employees, member financial institutions, business partners and/or the brand if revealed in error. The vast majority of Reflektive information assets fall into this category.

- **Public** – This classification applies to information assets approved by Reflektive management for release to the public. There is no concern of unauthorized disclosure, and the information asset may be freely disseminated without potential harm.

Authorities

ISO 27001 A.8.2.1; SOC 2: CC2.2, CC2.3, CC3.1, CC3.2, CC5.1, CC7.1, C1.1

7.2.2 Labeling of Information

Policy

Information must be identified and labeled, when appropriate in accordance with the assigned information security classification.

Explanation

To protect information in accordance with its security classification.

Standard

Create labels on information that are easily recognizable with the assigned information security classification. An information label section on company correspondence shall guide the placement of labeling.

Authorities

ISO 27001 A.8.2.2; SOC 2: CC2.2, CC2.3, CC3.1, CC3.2, CC5.1, CC7.1, C1.1

7.2.3 Handling of Assets

Policy

Assets must be handled, processed, stored and communicated in accordance with the assigned information security classification.

Explanation

To protect information in accordance with its security classification.

Standard

Review the information classification scheme and define protections for each. Defining how assets are handled shall consider:

- Access restrictions of each classification scheme;
- Log maintenance of authorized asset recipients; and
- Manufacturer specifications for storage of IT assets.

The classification scheme of other organizations may not be equivalent to Reflektive classification scheme despite similar terminology. Therefore agreements with external parties shall align how assets are classified and handled.

Authorities

ISO 27001 A.8.2.3; SOC 2: CC2.2, CC2.3, CC3.1, CC3.2, CC5.1, CC7.1, C1.1

7.3 Media Handling

To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

7.3.1 Disposal of media

Policy

Media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.

Explanation

To ensure that information cannot be retrieved from media that is no longer in use.

Standard

Media containing confidential information must be securely stored and disposed of by:

- Incineration, shredding, or erasure of data for use by another application within the organization; or
- Use of approved vendor offering disposal services and certificate of secure media destruction.

Asset management must maintain a log of media disposal.

Authorities

ISO 27001 A.8.3.2; SOC 2: CC2.2, CC2.3, CC3.2

8 Access Control

8.1 Business Requirements of Access Control

To limit access to information and information processing facilities.

8.1.1 Access Control Policy

Policy

Access to information systems and services must be consistent with business needs and be based on security requirements.

Explanation

To ensure that information and information systems are available for authorized use and protected from unauthorized use.

Standard

Access to all users, systems, and programs shall be restricted based on the principles of “least privileges” and “need to know”:

- Users shall be granted “least privileges” required to accomplish their tasks;
- Applications shall be implemented with “least privileges” to perform their functions;
- General support systems shall be granted the “least privileges” to fulfill their role in the network;
- Assignment of privileges shall be based on an individual’s job classification and function;
- The access shall be provided only if it is required as per business requirement;
- Approval by authorized parties specifying required privileges must be documented; and
- Access controls are enforced by an automated system.

Authorities

ISO 27001 A.9.1.1; SOC 2: CC3.2, CC5.1, CC5.2, CC5.3, CC5.4, CC5.5, CC5.6, C1.3

8.1.2 Access to Networks and Network Services

Policy

Users must only be provided access to the information systems they have been specifically authorized to use.

Explanation

To support the information system access control policy by limiting network access to authorized users of specific information systems.

Standard

Users shall only be provided with access to the services that they have been specifically authorized to use. Control includes:

- Access to all network and security devices shall be restricted to specific individuals in the organization;
- Authorization procedures for determining who is allowed to access to which networks and network services, consistent with other access rights;
- Policies on deployment of technical controls to limit network connections; and
- An examination and evaluation shall be required on a half-yearly basis for:
    - Changes or modifications made to the devices; and
    - User ID and privilege management for the devices.

Authorities

ISO 27001 A.9.1.2; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4, CC5.6, CC5.7

8.2 User Access Management

To ensure authorized user access and to prevent unauthorized access to systems and services.

8.2.1 User Registration and De-registration

Policy

There must be a formal user registration and de-registration process for granting access to all information systems.

Explanation

To ensure that all access actions are traceable to an identifiable individual or process.

Standard

To the extent possible, user IDs will be assigned to individuals and be named such that the individual is readily identifiable. Common or generic user IDs (used by more than one individual) are discouraged unless there is a compelling reason that individual accounts cannot be used. Common or generic user IDs must be approved by IT management.

Authorities

ISO 27001 A.9.2.1; SOC 2: CC5.2, CC5.4

8.2.2 User Access Provisioning

Policy

Access to systems and services must be consistent with business needs and be based on security requirements.

Explanation

To limit users' access to that which is necessary.

Standard

Reflektive will define and document access control rights and rules for each user or group of users. Service providers shall be given clear statements of the business requirements met by these access controls. Access to information and information services will only be given on the basis of business and security requirements.

Access will be given on a need to know basis, based upon the security requirements and business requirements of individual business applications. Access to information shall be provided in a manner that aims to protect the confidentiality and integrity of that information and without compromise to associated information or raw data.

Access will be given that is consistent with security levels and classifications, consistent with legislation and contractual obligations for confidentiality.

Access to standard common groups of users will be given standard access profiles. Access rights in a networked environment will recognize all connection types available. All users and groups of users shall receive a clear statement as to the access policy and as to the requirements met by these access controls.

Administrator access to production systems will be limited to only those with a justified business requirement for such access. Developers and other application personnel will not have access to the underlying operating system on production systems, except in emergencies and then with access only granted for the time necessary. System administrators shall not have access to the applications if possible.

Authorities

ISO 27001 A.9.2.2; SOC 2: CC5.2, CC5.4

8.2.3 Management of Privileged Access Rights

Policy

The allocation and use of system privileges must be restricted and controlled.

Explanation

To prevent misuse of these accounts – either accidentally or intentionally that can result in significant harm to the Reflektive environment.

Standard

All privileges shall be granted only with formal authorization. This authorization shall be accomplished along with User ID authorization, according to IT guidelines. All privileges that are granted will be documented. No privileges shall be granted until authorization is complete.

Elevated privileges (Administrator or root, etc.) should be assigned to a different user ID than that used for normal business use. Administrators should only use their elevated privilege accounts when conducting activities that actually require them. Elevated privileges must only be assigned to dedicated systems administrators and not normal users.

Records of these authorized and privileged accounts must be reviewed and maintained.

Authorities

ISO 27001 A.9.2.3; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4, CC5.8

8.2.4 Management of Secret Authentication Information of Users

Policy

The allocation of secret authentication information must be controlled through a formal management process.

Explanation

To ensure that access to information systems through secret authentication information is protected.

Standard

Allocation of secret authentication information shall be controlled through a formal management process. This includes user passwords and access token management. Control includes:

- All users shall keep personal secret authentication information confidential;
- All users shall have a unique identifier (user ID) for their personal and sole use for access to all computing services;
- The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason;
- Where users are required to maintain their own passwords, system/application administrators shall provide them with a secure initial temporary password, which they are forced to change immediately;
- Temporary passwords shall be given to users in a secure manner;
- Temporary passwords provided when users forget their password shall only be supplied following positive identification of the user;
- Passwords shall never be stored on computer systems in an unprotected manner; and
- Secret authentication information management procedures shall be put into place to ensure the implementation of the requirement of the Information Security Policy and to assist users in complying with best practice guidelines.

Authorities

ISO 27001 A.9.2.4; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4

8.2.5 Review of User Access Rights

Policy

Information Owners and Information Custodians must formally review user access rights at regular intervals.

Explanation

To ensure that access rights only exist for users with a defined “need to know”.

Standard

User accounts will be reviewed by the CISO and Human Resources on a quarterly basis. Accounts will include both active employee and contractors.

Authorities

ISO 27001 A.9.2.5; SOC 2: CC3.1, CC5.1

8.2.6 Removal or Adjustment of Access Rights

Policy

The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

Explanation

To ensure physical and logical access rights to information systems and information processing facilities are managed in relation to the security responsibilities of the job requirements.

Standard

Upon termination notification from HR, access to all Reflektive IT managed systems are disabled on or within twenty-fours hours of the effective termination date.

Accounts of terminated personnel with privileged access must be disabled immediately.

Authorities

ISO 27001 A.9.2.6; SOC 2: CC3.1, CC5.1, CC5.2, CC5.4

8.3 User Responsibilities

To make users accountable for safeguarding their authentication information.

8.3.1 Use of Secret Authentication Information

Policy

Users must follow good security practices in the selection and use of secret authentication information.

Explanation

To maintain the integrity of the unique identifier (user ID) by ensuring users follow good security practices.

Standard

Users must agree to their security responsibilities in their terms and conditions of employment. All users must adopt the following guidelines for allocating and managing their passwords:

- Allocate unique passwords;
- Keep passwords confidential;
- Avoid keeping a paper record of passwords;
- Change passwords whenever there is any suspicion of possible system or password compromise;
- Select passwords with a minimum length of nine characters and including both alphabetic and numeric characters;
- Avoid basing passwords on any of the following:
  - Month of the year, days of the week or any other aspect of the date
  - Family names, initials or car registration numbers
  - Company names, identifiers or references
  - Telephone numbers or similar all numeric groups
  - User ID, username, group ID or other system identifier
  - More than two consecutive identical characters
- Avoid reusing or cycling old passwords;
- Change passwords for privileged accounts at appropriate times;
- Change an initially allocated temporary password the first time they log on;
- Not to share individuals' user codes and passwords, or permit another user to use their user code for access.

Authorities

ISO 27001 A.9.3.1; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4

8.4 System and Application Access Control

To prevent unauthorized access to systems and applications.

8.4.1 Information Access Restriction

Policy

Access to information systems functions and information must be restricted in accordance with the access control policy.

Explanation

To restrict access to application systems functions and information to authorized individuals or systems.

Standard

Access to all users, systems, and programs shall be restricted based on the principle of "least privileges" and "need to know":

- Users shall be granted “least privileges” required to accomplish their tasks;
- Applications shall be implemented with “least privileges” to perform their functions;
- General support systems shall be granted the “least privileges” to fulfill their role in the network;
- Assignment of privileges shall be based on an individual’s job classification and function;
- The access shall be provided only if it is required as per business requirement;
- Approval by authorized parties specifying required privileges must be documented; and
- Access controls are implemented by an automated system.

Authorities

ISO 27001 A.9.4.1; SOC 2: CC3.2, CC5.1, CC5.2, CC5.3, CC5.4, CC5.5, CC5.6, C1.3

8.4.2 Secure Log-on Procedures

Policy

Access to systems and applications must use a secure log-on process.

Explanation

To ensure access to systems and applications are limited to authorized users and processes.

Standard

All users shall be identified and authenticated with the minimum of a unique identification and a password before access to operating systems is granted. This will minimize the opportunity for unauthorized access to information resources at the operating system level by providing a means of user authentication. If access to the operating system is not necessary, such as when the user has access to an application (only) running on the system, then operating system access must not be given to the user.

If operating system access is necessary, such access will abide by the following rules:

- All users shall have a unique user account
- All users shall have a unique password
- Users’ passwords will give no indication to their privilege level

Authorities

ISO 27001 A.9.4.2; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4, CC5.6, CC5.7

8.4.3 Password Management System

Policy

A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.

Explanation

To support the operating system access control policy through use of password management systems to enforce the password standard.

Standard

All passwords for systems and applications must be individual, effective, and of sufficient quality to deter compromise. Systems and applications must be configured to programmatically enforce these rules if available. In the absence of programmatic enforcement, the user will be responsible for enforcing these rules themselves.

The following minimum password requirements must be enforced:

- Eight characters or more; AND
- At least one of the following categories of characters:
    - Mixed case
    - Number
    - Special character

Authorities

ISO 27001 A.9.4.3; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4

8.4.4 Use of Privileged Utility Programs

Policy

Use of system utility programs must be restricted and tightly controlled with role-based access controls.

Explanation

To restrict and tightly control the use of utility programs, which may be used to override system and application controls.

Standard

Allocate privileged accounts on a need-to-use basis and on an event-by-event basis based on the minimum requirement for their functional roles. Assign a special and unique user ID for privileged activities separate from regular business activities.

For generic administration user IDs that are shared, passwords should be changed frequently and immediately when a privileged user is terminated. These changes must be communicated to relevant parties.

Records of these authorized and privileged accounts must be reviewed and maintained.

Authorities

ISO 27001 A.9.4.4; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4, CC5.8

8.4.5 Access Control to Program Source Code

Policy

Access to program source code must be restricted in accordance with the access control policy.

Explanation

To restrict access to program source code to authorized individuals or systems.

Standard

To prevent damage to Reflektive systems and applications, Reflektive will actively protect its information assets from covert channels and Trojan code.

The organization will follow the following procedures when acquiring software:

- All programs will be acquired from reputable sources
- All programs that are acquired will have source code verified
- All products shall have source code inspected prior to operational use

Access shall be that which is allowed in Reflektive's access control policy.

Modification to code, if necessary, shall be controlled, monitored, inspected, and only done by those staff members that have proven their trustworthiness to work on key systems.

Authorities

ISO 27001 A.9.4.5; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4, CC5.8

9 Cryptographic Controls

Control

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

9.1.1 Policy on the Use of Cryptographic Controls

Policy

The use of cryptographic controls must be based on the risk of unauthorized access and the classification of the information or information system that is to be protected.

Explanation

To manage the use of cryptography for protecting the confidentiality and integrity of electronic information.

Standard

Assess the risk and the sensitivity of information to determine the level of cryptographic controls necessary. Upon business need, cost analysis and legal restrictions, management must approve the appropriate level of encryption.

- If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases); and
- Decryption keys must not be tied to user accounts.

Specifications shall be based on a thorough risk assessment that includes appropriate algorithm selections, key management and other core features of cryptographic implementations.

Strong cryptography and security protocols shall be used to safeguard sensitive data during transmission over open, public networks. Wireless networks transmitting such data shall use industry best practices to implement strong encryption for authentication and transmission. Controls shall address, as appropriate, application to data at rest and fixed-location devices, data transported by mobile/removable media and embedded in mobile devices, and data transmitted over communications links.

Authorities

ISO 27001 A.10.1.1; SOC 2: CC5.7, C1.1

9.1.2 Key Management

Policy

A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls.

Explanation

To provide trustworthy key management processes for Reflektive cryptographic services.

Standard

Cryptographic keys must be stored securely and in the fewest possible locations and forms. All keys shall be protected against modification and destruction. Secret and private keys need protection against unauthorized disclosure. Cryptographic techniques may be used for this purpose. Physical protection shall be used to protect equipment used to generate, store and archive keys.

Procedures should be documented and address:

- Generation of strong cryptographic keys;
- Distributing, storing, archiving and changing/updating keys;
- Recovering, revoking/destroying and dealing with compromised keys;
- Retirement or replacement of cryptographic keys; and

- Logging all transactions associated with keys.

Authorities

ISO 27001 A.10.1.2; SOC 2: CC5.7, C1.1

10 Physical and Environmental Security

10.1 Secure Areas

To prevent unauthorized physical access, damage and interference to the organization's information.

10.1.1 Physical Security Perimeter

Policy

Reflektive office space must be protected by a defined physical security perimeter.

Explanation

To prevent unauthorized physical access to Reflektive information

Standard

Security perimeters should be used to protect areas that contain information and information processing facilities – using walls, controlled entry doors, manned reception desks and other measures.

- Secure areas must be designated that effectively restrict and limit access to sensitive information resources;
- Perimeter walls, floors, and ceilings must be resistant to normal attempts at forced entry;
- Barriers, alarms and monitoring systems must be able implemented to immediately detect and prevent attempted forced entry;
- Access to secure areas shall be monitored and controlled through an access control list of authorized personnel. IT Manager would be responsible for additions, deletions, or changes to the lists;

Authorities

ISO 27001 A.11.1.1; SOC 2: CC3.2, CC5.1, CC5.2, CC5.3, CC5.4, CC5.5

10.1.2 Physical Entry Controls

Policy

Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Explanation

To prevent unauthorized physical access to Reflektive information.

Standard

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Control includes:

- Entry shall be provided to authorize personnel only;
- Access control mechanisms shall be used to monitor individual physical access to sensitive areas;
- Data from access control mechanisms should be reviewed and correlated with other entries and stored for at least 3 months, unless otherwise restricted by law;
- The physical access control system shall be controlled and managed by the IT department and an inventory of all access will be maintained.

Authorities

ISO 27001 A.11.1.2; SOC 2: CC3.2, CC5.1, CC5.2, CC5.3, CC5.4, CC5.5

10.1.3 Securing Offices, Rooms and Facilities

Policy

Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility. The operation of information processing facilities on behalf of Reflektive or Reflektive's cloud vendors must be accredited under ISO 27001, SOC 2 and/or other certifications with relevant physical security requirements.

Explanation

To enhance physical and environmental security of information processing facilities by considering all security requirements during the design of the facility.

Standard

Secure offices, rooms and facilities from unauthorized access, damage, and interference through key or badge access. The protection should be commensurate with the identified risks. Any information processing facilities which operate with ISO 27001 and/or SOC 2 accreditation are presumed to meet this standard.

Authorities

ISO 27001 A.11.1.3; SOC 2: CC3.2, CC5.1, CC5.2, CC5.3, CC5.4, CC5.5

10.1.4 Protecting Against External and Environmental Threats

Policy

Physical security controls must be designed to protect against damage from natural or manmade disaster.

Explanation

To enhance physical and environmental security by designing and applying physical security controls to protect against damage from natural or man-made disaster.

Standard

Physical protection, recovery plans and contingency plans shall be designed and implemented to protect against natural and human threats. Review facility insurance policies and the protection they provide against natural or man-made threats.

Authorities

ISO 27001 A.11.1.4; SOC 2: CC3.2, CC3.3, A1.1, A1.2

10.2 Unattended User Equipment

Policy

Users must ensure unattended equipment has appropriate protection.

Explanation

To reduce risk of unauthorized access, loss or damage to information and information systems.

Standard

Equipment installed in user areas, such as workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period. All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protections.

- The use of time out software protection;
- Screensavers that require the use of a password to continue;
- Logging out of sessions when the session is finished;
- Logging out of sessions if the computer is left for more than 15 minutes; and
- Wherever sensible, switch off computers when not in use.

Authorities

ISO 27001 A.11.2.8, A.11.2.9; SOC 2: CC2.3, CC3.2

10.2.1 Clear Desk and Clear Screen Policy

Policy

Users must ensure the safety of sensitive information located on their desks or displayed on their screens from unauthorized access, loss or damage.

Explanation

To reduce risk of unauthorized access, loss or damage to information by ensuring users take reasonable security precautions.

Standard

Users must take reasonable security precautions to not leave sensitive information in clear view on their desks or screens. Sensitive information should be locked away in drawers when left unattended. Unattended user equipment standards apply to clear screen standards as well:

- The use of time out software protection;
- Screensavers that require the use of a password to continue;
- Logging out of sessions when the session is finished;
- Logging out of sessions if the computer is left for more than 15 minutes; and
- Wherever sensible, switch off computers when not in use.

Authorities

ISO 27001 A.11.2.9; SOC 2: CC2.3, CC3.2

11 Operations Security

11.1 Operational Procedures and Responsibilities

To ensure the correct and secure operation of information processing facilities.

11.1.1 Documented Operating Procedures

Policy

Operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented and maintained.

Explanation

To ensure correct operations of information systems and information processing facilities.

Standard

Share documented operational procedures associated with information processing and communication facilities on the company intranet including:

- Operational security procedures that are consistent with the requirements in this security policy (e.g., user account maintenance and log review procedures);
- Documentation of/for all significant system activities including deployments and maintenance;
- Treatment of such documentation as a formal organizational record, subject to appropriate change authorization, change tracking and archiving; and

- Provision of appropriate security for such documentation, including distribution control.

Authorities

ISO 27001 A.12.1.1; SOC 2: CC2.3, CC3.2

11.1.2 Change Management

Policy

Changes to production infrastructure, manual changes to production data, production code changes, and changes to application code are subject to the Change Management process and must be appropriately defined, documented, tested (as applicable), and authorized prior to production implementation.

Explanation

To ensure changes to the operational environment are applied correctly and do not compromise the security of information and information systems.

Standard

There shall be a formal approval for proposed changes (that could potentially impact the production environment) that will be developed by Engineering Management.
Prior to any operational change there shall be an assessment that:

- Identifies significant changes;
- Records significant changes;
- Assesses the potential impact of such changes; and
- Procedures and responsibilities for aborting and recovering from unsuccessful changes.

Significant changes shall be communicated to all relevant persons.

Authorities

ISO 27001 A.11.1.2; SOC 2: CC2.6, CC3.1, CC3.2, CC5.1, CC7.1, CC7.2, CC7.3, CC7.4, C1.6

11.1.3 Capacity Management

Policy

The use of information system resources must be monitored, optimized and projections made of future capacity requirements.

Explanation

To reduce the risk of system failures and unacceptable performance levels by monitoring and optimizing resources to meet current and future information system capacity requirements.

Standard

To limit disruption to the network, applications, and business functions, Reflektive will monitor system capacity and plan for future capacity needs in sufficient time to procure system resources prudently. This will ensure adequate resources are available and reduce the possibility of system overload.

System owners shall monitor their equipment for current uses and projected capacity.

Authorities

ISO 27001 A.12.1.3; SOC 2: CC3.2, CC4.1, A1.2

11.1.4 Separation of Development, Testing and Operational Environments

Policy

Development and testing information systems must be separated from operational information systems.

Explanation

To reduce the risk of unauthorized or inadvertent changes to operational information systems or information systems under development or being tested.

Standard

Test changes to operational systems and applications in a testing or staging environment prior to being applied to operational systems. Limit access to compilers, editors and other development tools or system utilities when not required. The environments must be segregated by the most appropriate controls including:

- Running on separate computers;
- Running on different domains; and
- Different usernames and passwords.

Authorities

ISO 27001 A.12.1.4; SOC 2: CC7.4

11.2 Protection from Malware

To ensure that information and information processing facilities are protected against malware.

11.2.1 Controls Against Malware

Policy

Security awareness, prevention and detection controls must be utilized to protect information systems against malware.

Explanation

To protect the integrity of information systems and software through requirements for the prevention and detection of malware.

Standard

Anti-malware software must be installed and maintained on all workstations and servers and provided on appropriate points on the network. The software must be from an established vendor with consistent results in recognizing and removing malware. All updates must be installed as soon as they are available. Users must not bypass, turn off or disable anti-malware software.

A regular review of all business critical systems must be conducted to identify all software running on the systems. Any unauthorized files or software must be formally investigated and, if appropriate, deleted.

All workstation software must be approved and installed by IT. Software must also be controlled to ensure compliance with licensing requirements.

Malware can be introduced through hoax emails and users must be vigilant to guard against this. Users must report the email to IT. All email attachments should be checked for malware at the point of entry onto the network.

Authorities

ISO 27002 12.2.1; SOC 2: CC5.8

11.3 Backup

To protect against loss of data.

11.3.1 Information Backup

Policy

Information and information systems must be backed up and the recovery process tested regularly to ensure that mission critical data and archives are adequately preserved and protected against data loss and destruction.

Explanation

To maintain the availability and integrity of information resources in the case of failure or disaster, by retaining up-to-date back-ups that are stored at a distance sufficient to escape damages that might occur at the main site.

Standard

Reflektive will regularly back-up adequate copies and generations of all software, documentation and business information and store it off-site. Reflektive's back up strategy will include daily backups of customer information and retention of daily backups

for a thirty-day rolling window. Regular testing will be done to insure the quality and usability of backed-up resources.

Restoration procedures will be documented and tested to ensure that they are effective and comply with restoration time requirements. Restoration procedures shall be kept with the back-up copies at the remote location.

Back-up media shall be tested semi-annually to ensure the back-up can be relied upon. Operations shall be responsible for ensuring that back-ups are tested.

Authorities

ISO 27001 A.12.3.1; SOC 2: A1.2, A1.3

11.4 Logging and Monitoring

To record events and generate evidence.

11.4.1 Event Logging

Policy

Event logs recording user activities, exceptions, faults and information security events must be produced and kept and regularly reviewed.

Explanation

To ensure usage of information systems can be monitored and audited.

Standard

Administrators of systems, networks and applications are responsible for ensuring that event logging is enabled, configured properly and active. Logging systems must be able to identify affected resources and associated actions while protecting sensitive privacy data. Administrators must regularly review logs for suspicious activity and maintain evidence that logs have been reviewed.

Authorities

ISO 27001 A.12.4.1; SOC 2: CC4.1, CC5.1, CC5.2, CC5.3, CC5.4, CC5.5, CC5.6, CC6.2, CC7.4, C1.2

11.4.2 Protection of Log Information

Policy

Information system logging facilities and log information must be protected against tampering and unauthorized access.

Explanation

To preserve the integrity of information system logging facilities and log information.

Standard

Restrict access to logs and audit trails to authorized personnel. Where possible, segregate duties so system administrators do not have permission to erase or de-activate logs of their own activities.

Authorities

ISO 27001 A.12.4.2; SOC 2: CC3.2, CC5.6

11.4.3 Administrator and Operator Logs

Policy

Activities of privileged users must be logged, and the log must be subject to regular independent review.

Explanation

To protect Reflektive information from unauthorized access, modification or deletion.

Standard

Operations will regularly review the results of system logs to detect deviations from the access policy and address critical issues that deviate.

The factors that determine the frequency of review include:

- Value, criticality or sensitivity of the information or application involved;
- Past experience of infiltration or misuse; and
- Extent of interconnections.

Violators are subject to disciplinary action. Incidents shall be reviewed and controls put in place to stop future occurrences.

Authorities

ISO 27001 A.12.4.3; SOC 2: CC5.1, CC5.2, CC5.3, CC5.4

11.4.4 Clock Synchronization

Policy

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

Explanation

To ensure the integrity of information system logs.

Standard

All critical system clocks must be synchronized with a Reflektive approved NTP service.

Authorities

ISO 27001 A.12.4.4; SOC 2: CC6.2

11.5 Control of Operational Software

To ensure the integrity of operational systems.

11.5.1 Installation of Software on Operational Systems

Policy

The implementation of software on operational information systems providing services must be controlled.

Explanation

To prevent compromise of operational information systems providing services from unauthorized software installation.

Standard

Procedures shall be implemented to control the installation of software on operational systems, to minimize the risk of interruptions in or corruption of information services. Control includes:

- Updating performed only with appropriate management authorization;
- Updating performed only by appropriately trained personnel;
- Only appropriately tested and certified software deployed to operational systems;
- Appropriate change management and configuration control processes for all stages of updating;
- Appropriate documentation of the nature of the change and the processes used to implement it;
- A rollback strategy in place, including retention of prior versions as a contingency measure; and
- Appropriate audit logs maintained to track changes.

Authorities

ISO 27001 A.12.5.1; SOC 2: CC5.8, CC7.1

11.6 Technical Vulnerability Management

To prevent the exploitation of technical vulnerabilities.

11.6.1 Management of Technical Vulnerabilities

Policy

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

Explanation

To mitigate damage to Reflektive operations resulting from exploitation of published vulnerabilities.

Standard

Timely information about technical vulnerabilities of information systems used by the organization shall be obtained, evaluated in terms of organizational exposure and risk, and appropriate countermeasures taken.

- A complete inventory of information assets sufficient to identify systems put at risk by a particular technical vulnerability;
- Procedures to allow timely response to identification of technical vulnerabilities that present a risk to any of the organization's information assets, including a timeline based on the level of risk; and
- Defined roles and responsibilities for implementation of countermeasures and other mitigation procedures.

<u>Security Patches</u>
All system components and software should be maintained and protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Critical security patches should be installed within a time frame commensurate with risk. If a risk-based approach is used to prioritize patch installation, critical devices and systems should be addressed within two months and less critical devices and systems may be addressed within three months.

<u>Public-facing Web Applications</u>
For public-facing web applications, new threats and vulnerabilities should be addressed on an ongoing basis. These applications should be protected against known attacks.

- Review of public-facing web applications via manual or automated application vulnerability security assessment tools or methods at least annually or after any changes;
- Verify that vulnerabilities are corrected;
- Re-evaluate the application after corrections; and
- Install a web-application firewall in front of public-facing web applications.

<u>Penetration Testing</u>
External and internal penetration testing should be performed at least once a year and after any significant infrastructure or application upgrade or modification, including but not

limited to after an operating system upgrade, a sub-network added to the environment, or a web server added to the environment.

Tests should be performed by a qualified internal resource or qualified external third party. Noted exploitable vulnerabilities should be corrected and testing repeated. Penetration tests should include application-layer penetration tests and network-layer penetration tests, including components that support network functions and operating systems.

Authorities

ISO 27001 A.12.6.1; SOC 2: CC4.1, CC5.6, CC5.8, CC7.1, CC7.2

12 Communications Security

12.1 Network Security Management

To ensure the protection of information in networks and its supporting information processing facilities.

12.1.1 Network Controls

Policy

A range of controls must be implemented to achieve and maintain security within the Reflektive network.

Explanation

To ensure that network security controls and network security management practices are implemented and documented to protect the network infrastructure, information traversing the network, and network-attached information systems.

Standard

Networks shall be appropriately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit and at rest. Control includes:

- Establishment of responsibilities and procedures for management of equipment on the network, including equipment in user areas;
- Special controls to safeguard the confidentiality and integrity of sensitive data passing over the organization's network and to/from public networks;
- Appropriate logging and monitoring of network activities, including security-relevant actions; and
- Management processes to ensure coordination of and consistency in the elements of the network infrastructure.

Authorities

ISO 27001 A.13.1.1; SOC 2: CC2.3, CC2.6, CC3.2, CC4.1, CC5.6, CC5.7, CC6.2

12.1.2 Security of Network Services

Policy

Security mechanisms, service levels and management requirements of all network services must be documented and included in any network service agreement.

Explanation

To specify what security mechanisms are required for delivery of a network service

Standard

Review the security arrangements of network service providers to ensure that they implement network services in a secure manner. Security features of network services could include:

- Application of authentication, encryption and network connection controls;
- Technical parameters required for secured connection with the network services;
- Procedures for the network service usage to restrict access to network services or applications, where necessary.

Authorities

ISO 27001 A.13.1.2 SOC 2: C1.4, C1.5

12.1.3 Segregation in Networks

Policy

Groups of information services, users and information systems must be segregated on networks.

Explanation

To isolate information systems, users and networks based on risk and business connectivity requirements to control information flow, minimize unauthorized connection attempts and limit the spread of damage in case of compromise.

Standard

Assess the security requirements of each network domain to determine the level of segregation and access necessary. Control includes:

- Separation into logical domains, each protected by a defined security perimeter;
- Secure gateways between/among logical domains;
- The network must be segregated into separate logical domains with routing and access controls operating between the domains; and
- The levels of control must be commensurate with the access policy requirements of the domains being interconnected.

Authorities

ISO 27001 A.13.1.3; SOC 2: CC5.6

12.2 Information Transfer

To maintain the security of information transferred within Reflektive and with any external entity.

12.2.1 Information Transfer Policies and Procedures

Policy

Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information through all types of communication services.

Explanation

To protect information from interception, copying, modification, misrouting and destruction.

Standard

Various types of communication facilities for information transfer include email, voice, facsimile and video. Consider the following when transferring information through all types of communication services:

- Procedures against interception, copying, modification, misrouting and destruction of transferred information;
- Procedures for detection and protection against malware transmitted through electronic communication;
- Use of cryptographic controls to protect the confidentiality, integrity and authenticity of information; and
- Avoiding confidential conversations in public or insecure communication channels.

Authorities

ISO 27001 A.13.2.1; SOC 2: CC5.7, CC7.4, C1.2

12.2.2 Agreements on Information Transfer

Policy

Information and software exchange agreements between Reflektive and other organizations must be documented.

For purposes of this policy, an “information exchange agreement” can mean one or more provisions within a larger agreement; e.g., an information exchange provision within a service agreement.

Explanation

To protect information or software from loss or unauthorized disclosure.

Standard

Information exchange agreements outline the roles, responsibilities, and data ownership between Reflektive and external parties. These agreements shall specify the security controls and conditions appropriate for the information that is shared, whether the information is shared or stored in electronic or physical form. The content of the agreement shall vary depending on the reason for the exchange.

The agreement, at a minimum, shall address the following:

- Management's responsibilities for controlling and notifying of transmission, dispatch and receipt;
- Procedures for notifying sender of transmission, dispatch and receipt;
- Responsibilities and liabilities in the event of loss of data;
- Information and software ownership and responsibilities for data protection, software copyright compliance, and similar considerations;
- Any special controls that may be required to protect sensitive items, such as cryptographic keys.

Authorities

ISO 27001 A.13.2.2; SOC 2: CC2.2, CC2.3, CC3.2, CC7.4, C1.2, C1.3

12.2.3 Electronic Messaging

Policy

Information transmitted by electronic messaging must be appropriately protected.

Explanation

To enable secure and trustworthy electronic messaging.

Standard

The organization will safeguard media or information in a manner commensurate with its data classification. Sensitive information shall be protected from unauthorized access or modification by methods that include use of credentials, digital signature and/or encryption.

Authorities

ISO 27001 A.13.2.3; SOC 2: CC5.7, CC7.4, C1.2

12.2.4 Confidentiality or Non-disclosure Agreements

Policy

A confidentiality agreement reflecting organizational requirements for the handling of information must be in place and reviewed regularly.

For purposes of this policy, a “confidentiality agreement” or “non-disclosure agreement” can mean one or more provisions in a larger agreement; e.g., a confidentiality provision within a service or employment agreement.

Explanation

To ensure personnel understand their role in maintaining the confidentiality of information and information systems.

Standard

Personnel must agree to their responsibility for information security in both confidential and non-disclosure agreements as well as in the terms and conditions of employment. Personnel must review confidentiality and non-disclosure agreements annually. Such agreements shall include:

- Definition of the information, information type(s) or information system(s) to be protected;
- Agreements for that information rendered in clear, legally-enforceable terms, that accord with all relevant statutory-regulatory and private certificatory authorities;
- Responsibilities of signatories, including limitations on use or disclosure of information and adherence to security controls;
- Terms of ownership of information, including any trade secret or intellectual property requirements;
- Expected duration of the agreement;
- Required actions when the agreement is terminated, including requirements to return or destroy information;
- Right to monitor compliance with the agreement;
- Processes for reporting of and notice of breaches; and
- Expected actions to be taken in the event of a breach.

Authorities

ISO 27001 A.13.2.4; SOC 2: CC2.2, CC2.3, CC7.4, C1.2, C1.3

13System Acquisition, Development and Maintenance

13.1 Security Requirements of Information Systems

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

13.1.1 Information Security Requirements Analysis and Specification

Policy

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Explanation

To integrate system security requirements into business processes supporting the development, maintenance and acquisition of information systems.

Standard

Identify information security requirements from various compliance requirements, incident reviews, or vulnerability thresholds. Results of the findings must be included during the early stages of information system projects.

Authorities

ISO 27001 A.14.1.1; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.1.2 Securing Application Services on Public Networks

Policy

Information involved in application services passing over public networks must be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Explanation

To protect applications accessible via public networks from a range of network related threats.

Standard

Security controls include encryption, authorization process, network security controls, checks and balances to verify transactions, and non-repudiation. Care should also be taken to verify the validity and integrity of publicly available information provided over the

Internet. Strong cryptography and security protocols should be used to safeguard sensitive data during transmission over open, public networks.

Authorities

ISO 27001 A.14.1.2; SOC 2: CC5.6, CC5.7

13.1.3 Protecting Application Services Transactions

Policy

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Explanation

To protect application service transactions.

Standard

Security controls include encryption, authorization process, network security controls, checks and balances to verify transactions, and non-repudiation. Care should also be taken to verify the validity and integrity of publicly available information provided over the Internet. Strong cryptography and security protocols should be used to safeguard sensitive data during transmission over open, public networks.

Authorities

ISO 27001 A.14.1.3; SOC 2: CC5.6, CC5.7

13.2 Security in Development and Support Processes

To ensure that information security is designed and implemented within the development lifecycle of information systems.

13.2.1 Secure Development Policy

Policy

Rules for the development of software and systems must be established and applied to developments within the organization.

Explanation

To develop a secure service, architecture, software and system.

Standard

Security approval shall be required for all key project phases (i.e. concept, requirements, testing). All new or upgraded systems must have their security requirements documented.

A risk assessment will be performed to evaluate the security requirements for new systems or upgrades.

The system owner will specify the security requirements of all new implementations prior to their final approval.

- The controls and requirements will reflect the sensitivity and business value of the information assets involved.
- Independent consultants will be brought in to assist in evaluations if deemed necessary.
- Vulnerability scans and/or penetration tests will be run against systems to ensure security controls are in place, patch levels are current, and unnecessary services are not running.

Authorities

ISO 27001 A.14.2.1; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.2.2 System Change Control Procedures

Policy

Changes to production systems must be controlled by the use of formal change control procedures.

Explanation

To ensure that information systems are not compromised from unauthorized changes.

Standard

The application owners shall be responsible for overseeing the security and control procedures of all changes to production applications. All software changes require formal approval by the application owner. All changes to software will be documented.

Application owners and the CISO shall be responsible for insuring that programmers are only given access to areas of the application that are necessary for the approved work.

Application owners shall oversee the entire application change process prior to change including:

- Maintaining a record of agreed upon authorization levels
- Ensuring changes are submitted by authorized users
- Performing risk assessment to assure that controls and integrity procedures will not be compromised by changes, that business interruption is kept to an acceptable minimum and that the timing is appropriate for the change
- Identifying all software, information, databases and hardware that require change
- Obtaining formal approval prior to work commencing

Application owners shall oversee the entire application change process during the change including:

- Ensuring change minimized business interruption
- Documentation is updated and old documentation is archived
- Version control is maintained
- Maintaining an audit log of all change requests
- Updating all user procedures

Authorities

ISO 27001 A.14.2.1; SOC 2: CC2.6, CC3.1, CC3.2, CC5.1, CC7.1, CC7.2, CC7.4, C1.6

13.2.3 Technical Review of Applications after Operating Platform Changes

Policy

Information systems must be reviewed and tested when operating platform changes occur.

Explanation

To ensure information systems will not be disrupted or compromised.

Standard

Application owners shall oversee the entire application change process after the change including:

- Ensuring that testing is done securely (in a test environment that is segregated from development and operational systems)
- Ensuring that implementation does not disrupt business processes

Authorities

ISO 27001 A.14.2.3; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.2.4 Secure System Engineering Principles

Policy

Secure engineering principles and procedures must be established, documented, maintained and applied to any information system implementation activities.

Explanation

To design security into all system layers within the engineering process.

Standard

Developers should seek industry best practices when establishing secure coding principles. Open Web Application Security Principles (OWASP) lists ten principles for secure coding:

1. Minimize attack surface area

   Every feature that is added to an application adds a certain amount of risk to the overall application. The aim for secure development is to reduce the overall risk by reducing the attack surface area.

2. Establish secure defaults

   There are many ways to deliver an “out of the box” experience for users. However, by default, the experience should be secure, and it should be up to the user to reduce their security – if they are allowed.

3. Principle of Least privilege

   The principle of least privilege recommends that accounts have the least amount of privilege required to perform their business processes. This encompasses user rights, resource permissions such as CPU limits, memory, network, and file system permissions.

4. Principle of Defense in depth

   The principle of defense in depth suggests that where one control would be reasonable, more controls that approach risks in different fashions are better. Controls, when used in depth, can make severe vulnerabilities extraordinarily difficult to exploit and thus unlikely to occur.

   With secure coding, this may take the form of tier-based validation, centralized auditing controls, and requiring users to be logged on all pages.

5. Fail securely

   Applications regularly fail to process transactions for many reasons. How they fail can determine if an application is secure or not.

6. Don’t trust services

   Many organizations utilize the processing capabilities of third party partners, who more than likely have differing security policies and posture than you. It is unlikely that you can influence or control any external third party, whether they are home users or major suppliers or partners.

   Therefore, implicit trust of externally run systems is not warranted. All external systems should be treated in a similar fashion.

7. Separation of duties

   A key fraud control is separation of duties. For example, someone who requests a computer cannot also sign for it, nor should they directly receive the computer. This prevents the user from requesting many computers, and claiming they never arrived.

   Certain roles have different levels of trust than normal users. In particular, administrators are different to normal users. In general, administrators should not be users of the application.

8. Avoid security by obscurity

Security through obscurity is a weak security control, and nearly always fails when it is the only control. This is not to say that keeping secrets is a bad idea, it simply means that the security of key systems should not be reliant upon keeping details hidden.

9. Keep security simple

Attack surface area and simplicity go hand in hand. Certain software engineering fads prefer overly complex approaches to what would otherwise be relatively straightforward and simple code.

Developers should avoid the use of double negatives and complex architectures when a simpler approach would be faster and simpler.

10. Fix security issues correctly

Once a security issue has been identified, it is important to develop a test for it, and to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all code bases, so developing the right fix without introducing regressions is essential.

Authorities

ISO 27001 A.14.2.5; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.2.5 Secure Development Environment

Policy

Organizations shall establish and appropriately protect secure development environments for system developmental and integration efforts that cover the entire system development lifecycle.

Explanation

To ensure people, processes and technology associated with system development and integration are secure.

Standard

Organizations should establish secure development environments for specific system development efforts, considering:

- Need for segregation between different development environments
- Control of access to the development environment
- Monitoring of change to the environment and code stored therein
- Backups are stored at secure offsite locations
- Control over movement of data from and to the environment

Authorities

ISO 27001 A.14.2.6; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.2.6 System Security Testing

Policy

Testing of security functionality shall be carried out during development.

Explanation

To ensure that system changes will not introduce vulnerabilities to the organization's environment.

Standard

All systems will be tested prior to acceptance, including a vulnerability assessment or scan prior to being permitted to connect to the Reflektive network. This process will ensure that security controls are in place and that the new system complies with the design and function required.

Authorities

ISO 27001 A.14.2.8; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.2.7 System Acceptance Testing

Policy

Acceptance testing programs and related criteria must be established for new information systems, upgrades and new versions.

Explanation

To ensure that system changes will not introduce vulnerabilities or disrupt the organization's environment.

Standard

All systems will be tested prior to acceptance, including a vulnerability assessment or scan prior to being permitted to connect to the Reflektive network. This process will ensure that security controls are in place and that the new system complies with the design and function required.

System owners shall ensure that the equipment capacity requirements are met prior to use of new system.

Managers and users (when applicable) shall inspect major new systems periodically throughout the development to ensure functionality is appropriate and compliant with design requirements.

Prior to the acceptance and use of new systems the following controls shall be documented and in place:

- The system is built according to standard hardware or software builds, published by IT
- Effective manual contingency procedures are documented (if applicable)
- Error recovery/restart procedures and contingency plans (if applicable)
- Updated business continuity plans (if applicable)
- Compatibility of new system to the security requirements of the organization
- Compatibility of the new system to the existing systems
- Security controls are in place and tested
- Vulnerability scan run against system to verify that patch levels are current and that no unnecessary services are running.

Users shall be adequately trained prior to taking a new system into operational mode. Operational testing procedures shall be documented and preparation for new system completed prior to acceptance. Systems must meet acceptance criteria, or have formal exceptions authorized, before being connected to the Reflektive network.

Note that these requirements do not apply to any system not connected to the Reflektive corporate network. This includes stand-alone systems, or systems in labs not connected to the rest of the network. If these systems are subsequently brought out of that environment and the desire is to connect them to the Reflektive network, then these requirements apply once again.

Authorities

ISO 27001 A.14.2.9; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

13.3 Test Data

To ensure the protection of data used for testing.

13.3.1 Protection of Test Data

Policy

Test data shall be selected carefully, protected and controlled.

Explanation

To protect operational data containing personally identifiable and other confidential information.

Standard

Test data shall be scrubbed of personally identifiable information. If test data cannot be scrubbed, then access controls in the test environment must be at the same level of protection as production.

Authorities

ISO 27001 A.14.3.1; SOC 2: CC3.2, CC7.1, CC7.2, CC7.4

14 Supplier Relationships

14.1 Information Security in Supplier Relationships

To ensure protection of the organization's assets that is accessible by suppliers. For purposes of this Information Security Policy, "suppliers" may refer to vendors and service providers that support production systems.

14.1.1 Information Security Policy for Supplier Relationships

Policy

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets must be agreed with the supplier and documented.

Explanation

To ensure that suppliers comply with the information security requirements of the organization.

Standard

The Chief Information Security Officer will control authorization for *types* of access to information processing facilities by third parties based upon the reasons for that access. A risk assessment will be carried out before any third party access is granted and will consider the reasons for access as well as the necessary controls to be put in place. Access of third parties to Information Processing facilities will be clearly spelled out in contracts; this access includes the scope of access to physical, logical and network assets.

Authorities

ISO 27001 A.15.1.1; SOC 2: CC3.2, , CC2.2, C1.3

14.1.2 Addressing Security within Supplier Agreements

Policy

All relevant security requirements must be established and agreed with each supplier that may access, process, communicate, or provide IT infrastructure components for, the organization's information.

Explanation

To ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

Standard

Any disclosure of confidential information to consultants, contractors, temporary employees, or any other third parties shall be preceded by the receipt of a signed non-disclosure agreement (NDA).

Access by third party contractors will be specifically agreed upon and documented in contracts.

Arrangements involving third party access to organizational information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with Reflektive security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party. Reflektive should satisfy themselves as to the indemnity of their supplier. The following terms should be considered for inclusion in the contract:

- The general policy on information security;
- Asset protection, including:
    - Procedures to protect organizational assets, including information and software;
    - Procedures to determine whether any compromise of the assets, i.e. loss or modification of data, has occurred;
    - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
    - Integrity and availability;
    - Restrictions on copying and disclosing information;
- A description of each service to be made available;
- The target level of service and unacceptable levels of service;
- Provisions for the transfer of staff where appropriate;
- The respective liabilities of the parties to the agreement;
- Responsibilities with respect to legal matters, i.e. data protection legislation, especially taking into account different national legal systems. If the contract involves cooperation with organizations in other countries
- Intellectual property rights (IPR's) and copyright assignment and protection of any collaborative work
- Access control agreements, covering:
    - Permitted access methods, and the control and use of unique identifiers such as user ID's and passwords;
    - An authorization process for user access and privileges;
    - A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with regard to such use;
- The definition of verifiable performance criteria, their monitoring and reporting;
- The right to monitor, and revoke, user activity;
- The right to audit contractual responsibilities or to have those audits carried out by a third party;
- The establishment of an escalation process for problem resolution, contingency arrangements should also be considered where appropriate;

- Responsibilities regarding hardware and software installation and maintenance;
- A clear reporting structure and agreed reporting format;
- A clear and specified process of change management;
- Any required physical protection controls and mechanisms to ensure those controls are followed;
- User and administrator training in methods, procedures and security;
- Controls to ensure protection against malicious software
- Arrangements for reporting, notification and investigation of security incidents and security breaches;
- Involvement of the third party with subcontractors.

These security requirements must address the confidentiality of Reflektive data and the third party's relationships with any Reflektive competitor. This is especially important when dealing with engineering partners who work with various companies in the same space as Reflektive.

Authorities

ISO 27001 A.15.1.2; SOC 2: CC3.2, , CC2.2, C1.3

14.1.3 Information and Communication Technology Supply Chain

Policy

Agreements with suppliers must include information security requirements associated with the information and communication technology supply chain.

Explanation

To ensure that the specific risks associated with information and communication technology supply chain matters are understood by both parties and mitigation requirements are included in the agreements.

Standard

See section 14.1.2.

Authorities

ISO 27001 A.15.1.3; SOC 2: CC2.2, CC3.2, C1.3

15Information Security Incident Management

15.1 Management of Information Security Incidents and Improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

15.1.1 Responsibilities and Procedures

Policy

Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.

Explanation

To enable quick and orderly management of information security incidents.

Standard

The CISO must clearly define the chain of command and responsibilities for handling information security incidents. Personnel assigned responsibility must receive proper training to respond to incidents.

The Incident Management Process includes details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited;
- Limiting or restricting further impact of the incident;
- Tactics for containing the incident;
- Corrective action to repair and prevent reoccurrence; and
- Communication to those affected.

Authorities

ISO 27001 A.16.1.1; SOC 2: CC2.5, CC3.2

15.1.2 Reporting Information Security Events

Policy

Information security events must be reported through appropriate management channels immediately.

Explanation

To enable prompt response to information security event(s) and identify company wide trends.

Standard

Communicate company wide responsibility to report information security events. Assign a point of contact to whom information security events may be reported. Situations that warrant reporting include:

- Ineffective security control;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors;
- Non-compliances with policies or guidelines;

- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware; and
- Access violations.

Authorities

ISO 27001 A.16.1.2; SOC 2: CC2.5, CC3.2, CC5.5, CC6.2

15.1.3 Reporting Security Weaknesses

Policy

Personnel using information systems must note and report any observed or suspected security weaknesses in those systems.

Explanation

To assist in maintaining the security of information systems all personnel must report observed or suspected security weaknesses in information systems.

Standard

All employees and contractors shall be educated on security breaches and escalation. All employees and contractors are required to note and report any observed or suspected security weaknesses in systems or services as soon as possible. They must not seek to exploit them to prove the weakness.

Security weaknesses can include:

- Inadequate firewall or antivirus protection;
- System malfunctions or overloads;
- Malfunctions of software applications; and
- Human errors.

Authorities

ISO 27001 A.16.1.3; SOC 2: CC2.5, CC3.2, CC5.5, CC6.2

15.1.4 Assessment of and Decision on Information Security Events

Policy

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

Explanation

To help identify the impact and extent of an incident.

Standard

Assign incident response teams that are trained to properly

- Collect evidence as soon as possible after the occurrence;

- Conduct information security forensic analysis;
- Escalate issues when necessary;
- Ensure that all involved response activities are properly logged for later analysis;
- Communicate the existence of the information security incident to relevant parties;
- Deal with issues found to cause or contribute to the incident; and
- Formally close and record incidents after they have been resolved.

Authorities

ISO 27001 A.16.1.4; SOC 2: CC2.5, CC3.2, CC5.5, CC6.2

15.1.5 Response to Information Security Incidents

Policy

Information security incidents must be responded to in accordance with the documented procedures.

Explanation

To ensure that incidents are responded to in a proper manner.

Standard

See section 15.1.4.

Authorities

ISO 27001 A.16.1.5; SOC 2: CC2.5, CC3.2, CC5.5, CC6.2

15.1.6 Learning from Information Security Incidents

Policy

Knowledge gained from information security incidents must be used to reduce the likelihood or impact of future incidents.

Explanation

To learn from information security incidents and to reduce future incidents.

Standard

Incidents must be recorded and a post-incident review conducted. The following details must be retained:

- Types of incidents;
- Volumes of incidents and malfunctions; and
- Impact of the incidents.

The information must be reviewed on a regular basis and assessed to identify any patterns or trends. Any changes to the process made as a result of the post-incident review must be formally noted.

Authorities

ISO 27001 A.16.1.6; SOC 2: CC3.2, CC6.2

15.1.7 Collection of Evidence

Policy

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Explanation

To ensure that evidence may be used for the purposes of disciplinary and legal action.

Standard

See section 15.1.4.

Authorities

ISO 27001 A.16.1.7; SOC 2: CC2.5, CC3.2, CC5.5, CC6.2

16 Information Security Aspects of Business Continuity Management

16.1 Information Security Continuity

Information security continuity should be embedded in the organization's business continuity management systems.

16.1.1 Planning Information Security Continuity

Policy

There must be a managed process to ensure that disaster recovery plans address information security requirements.

Explanation

To ensure Reflektive can continue to securely deliver essential services despite damage, loss, or disruption of business processes.

Standard

In the absence of formal disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization

could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

Authorities

ISO 27001 A.17.1.1; SOC 2: CC3.1, A1.2, A1.3

16.1.2 Implementing Information Security Continuity

Policy

Disaster recovery plans are developed to maintain and resume business operations to the required level following interruption to, or failure of, essential services.

Explanation

To ensure that essential services can be securely restored after the damage, loss, or disruption of business processes.

Standard

Establish, document, implement and maintain the following:

- Information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- Compensating controls for information security controls that cannot be maintained during an adverse situation.

Reflektive must test its disaster recovery and incident response plans annually or upon significant organizational or environmental changes to ensure continuing effectiveness.

Authorities

ISO 27002 17.1.2; SOC 2: CC3.1, A1.2, A1.3

16.2 Redundancies

To ensure availability of information processing facilities.

16.2.1 Availability of Information Processing Facilities

Policy

Redundant components or architecture must be implemented in information processing facilities to sufficiently meet availability requirements.

Explanation

To ensure availability of information systems through a redundant backup component when a system component fails.

Standard

Reflektive shall identify business requirements for availability of information systems. Consider using redundant components or architecture where availability cannot be guaranteed using the existing systems architecture.

Where applicable, redundant information systems supporting mission critical services should be tested to ensure failover from one component to another component within defined recovery objectives.

Authorities

ISO 27001 A.17.2.1; SOC 2: A1.2

17 Compliance

17.1 Compliance with Legal and Contractual Requirements

17.1.1 Identification of Applicable Legislation and Contractual Requirements

Policy

Legislative, regulatory and contractual requirements applicable to Reflektive's information systems and Reflektive's approach for conforming its information systems to those requirements must be explicitly identified, documented and maintained.

Explanation

To ensure that the legal and contractual requirements of Reflektive's information systems are documented.

Standard

Reflektive's personnel responsible for information systems shall seek the advice of Reflektive's legal counsel or Information Security Officers for all relevant legal and security information.

Care shall be taken to account for different requirements in different locations. Reflektive will consult its legal counsel to determine differences from standing policy for those locations that have differing legal requirements, and will work with the CISO to create exceptions to general policy and specific policies for those jurisdictions.

Authorities

ISO 27001 A.18.1.1; SOC 2: CC2.2, CC2.3, CC3.2, C1.4, C1.5

17.1.2 Intellectual Property Rights

Policy

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

Explanation

To avoid copyright infringement that can lead to legal action, which may involve fines and criminal proceedings.

Standard

Reflektive's personnel shall seek the advice of Reflektive's legal counsel or Information Security Officers for all relevant legal and security information.

Authorities

ISO 27001 A.18.1.2; SOC 2: CC2.2, CC2.3, CC3.2, C1.4, C1.5

17.1.3 Protection of Information System Records

Policy

Reflektive's information system records must be protected from loss, destruction, falsification, and unauthorized access/release.

Explanation

To ensure the Information Security Policy and supporting processes enable compliance with legal and policy requirements for Reflektive's information system records.

Standard

Any agency conducting system audits will protect access to system audit tools (i.e. software or data files). This will protect the security, availability and integrity of the organization's information resources by ensuring that the organization's system audit tools are protected from misuse or compromise.

System audit tools shall be separated from operational and development systems unless they are given additional, appropriate protection and are authorized for inclusion within operational and/or development systems by the CISO.

Employees must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance by the CISO.

Authorities

ISO 27001 A.18.1.3; SOC 2: CC3.2, CC5.6

17.1.4 Privacy and Protection of Personally Identifiable Information

Policy

Security controls must be applied to protect personally identifiable information in accordance with relevant legislation.

Explanation

To ensure the Information Security Policy and supporting processes enable compliance with legislation.

Standard

The CISO or a nominated information protection officer shall document policies and procedures that comply with applicable laws and regulations for the handling of personal information.

The CISO shall distribute policies and educate Reflektive's personnel on their responsibilities for compliance.

Information owners shall inform the CISO or appropriate information protection officer about proposals to keep information in a structured file which preserves the integrity of its information by tracking changes. The information protection officer shall advise information owners on policies and procedures concerning their protection and storage of such data.

Confidential information entrusted to Reflektive by customers, business partners, suppliers, and other third parties shall be protected in accordance with Reflektive Security Policies and shall be protected with at least the same care as Reflektive's confidential information.

Authorities

ISO 27001 A.18.1.4

17.1.5 Regulation of Cryptographic Controls

Policy

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

Explanation

To ensure compliance with relevant legislation and regulations on cryptographic controls.

Standard

System owners shall seek the advice of Reflektive's legal counsel or Information Security Officers for all relevant legal and security information.

Authorities

ISO 27001 A.18.1.4; SOC 2: CC2.2, CC2.3, CC3.2, C1.4, C1.5

17.2 Information Security Reviews

To ensure that information security is implemented and operated in accordance with Reflektive's policies and procedures.

17.2.1 Independent Review of Information Security

Policy

An independent review must be performed annually to ensure continued adherence to information security objectives and effectiveness of security controls.

Explanation

To ensure the continuing suitability, adequacy and effectiveness of Reflektive's approach to information security.

Standard

On an annual basis, management shall initiate an independent review of information security practices. Such a review shall be carried out by individuals independent of the area under review. The results of the independent review shall be recorded and reported to the management who initiated the review. Records of this reporting shall be maintained.

If the independent review identifies that the organization's approach and implementation to managing information security is inadequate and requirements are not met or not compliant with the direction for information security stated in the information security policies, management should consider corrective actions.

Authorities

ISO 27001 A.18.2.1; SOC 2: CC7.2

17.2.2 Compliance With Security Policies and Standards

Policy

Management must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.

Explanation

To ensure compliance of information systems with information security policy, requirements and standards.

Standard

Managers shall review how to apply security controls to their area of responsibility and consider how to apply reporting tools for efficient regular review. If managers discover any non-compliance, they should create a report to

- Identify the causes of the non-compliance;
- Evaluate the need for actions to achieve compliance;
- Implement appropriate corrective action;
- Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Authorities

ISO 27001 A.18.2.2, SOC 2: CC1.2

17.2.3 Technical Compliance Review

Policy

Information systems must be regularly checked for compliance with security policies and standards.

Explanation

To determine if technical controls meet established Reflektive standards.

Standard

Technical compliance shall be reviewed preferably with the assistance of automated tools. Alternatively, manual reviews by an experienced system engineer could be performed.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests shall be planned, documented, and repeatable.

Technical compliance review shall be carried by competent, authorized persons or under the supervision of such persons.

Authorities

ISO 27001 A.18.2.3; SOC 2: CC3.3, CC4.1