Information Security Policy

Minimal Requirements for

Information Security and IT Control

Date

July, 2018

Contents

0 Introduction

0.2 What is information security?

Information is an asset that, like other important business assets, is essential to Grupo Promax business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

1 Policy & Organization on Information Security

1.3 External Parties

Control Objective
To control the information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

1.3.1 Risks related to external parties

Control
Risks must be assessed before giving external parties access to information and information processing facilities.

Required considerations

a) Before an external party is allowed to access the information processing facilities or information of a Business Unit or the Corporate organization, a risk assessment is carried out to identify any requirements for specific controls.

b) In these risk assessments attention has been paid to at least:
   - The information and information facilities the external party has access to.
   - The type of access rights the external party has to information and information processing facilities.
   - Access is given on a ‘need to have’ basis (e.g. restricting data, systems, protocols, time).
   - Procedures for monitoring the access rights of external parties and deleting the access rights when no longer required.
   - Controls necessary to protect information that is not intended to be accessible by external parties.

c) Measures to mitigate risks must be implemented before granting external parties access.

d) Access must have expiration date.

1.3.2 Third Party Agreements

Control
Relevant security requirements and IT controls must be covered in agreements with third parties who access, process or manage information or information processing facilities (e.g. hosting).

Required Considerations

a) Security requirements and IT controls that follow from the risk assessment related to external parties must be reflected by a formal agreement with the external party.

b) In case (part of) IT services are outsourced, the Suppliers involved are obliged to comply with the Grupo Promax Information Security Policy, which it must be informed.

c) Periodically the implementation of the requirements and IT controls must be monitored (e.g. by means of a Third party Review) where deemed appropriate. In these cases the right for independent audits is built into the Third Party Agreements.

3 Human Resources IT Security

3.1 Responsibilities staff regarding information security

Control Objective
To ensure that employees, contractors and third party users understand their responsibilities regarding information security and to reduce the risk of theft, fraud or misuse of facilities.

3.1.1 IT Security Awareness

Control

All employees, contractors and third party users must be informed or trained to understand their responsibilities regarding the information security.

Required Considerations

a) Managers inform their employees, contractors and third party users on their responsibilities regarding the information security as relevant for their job function.

b) All new staff is informed on relevant information security policy statements and procedures.

c) Recurring security awareness activities must be performed to ensure that the behavior of staff is in accordance with the policies.

3.1.2 Confidentiality Agreement

Control

Employees, contractors and third party users are obliged to confidentiality requirements as part of their contractual obligation.

Required Considerations

a) Employees, contractors and third party users sign a confidentiality agreement as part of their contractual obligation. This can either be a separate confidentiality agreement or be part of an employment contract or third party contract.

4 Physical and Environmental Security

4.1 Physical access, damage and loss of information

Control Objective
To prevent unauthorized physical access, damage, loss and interference to information processing facilities, assets and activities.

4.1.2 Physical entry controls

Control
Information processing facilities must be protected by appropriate access controls to ensure that only authorized personnel are allowed access.

Required Considerations

a) Visitors to information processing facilities must be authenticated (e.g. using passport or driving license), supervised and name, date, time recorded.

b) Visitors must be only granted access for specific, authorized purposes.

4.1.3 Secure disposal or re-use of equipment

Control
Sensitive data and licensed software is properly removed before equipment is disposed or re-used.

Required Considerations

a) All IT storage media must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to being disposed or re-used.

5 Communications and Operations Management

5.1 Management of incidents and problems in the IT environment

Control Objective
To ensure that any incidents causing an interruption of services must be resolved in a timely and controlled manner.

5.1.1 Incident / problem management

Control
Incidents must be resolved in a timely and controlled manner and must be analyzed to determine and resolve structural problems.

Required Considerations

a) The incident / problem management procedures must be documented and followed to ensure that incidents must be recorded, analyzed and resolved in a timely manner.

b) At least the following is recorded for each incident:
  - the date of the incident;
  - the IT components involved;
  - the symptoms and characteristics of the incident;
  - the status of the incident (e.g. open, closed);
  - if the status is ‘closed’: a description of the solution.

c) In case solving incidents / problems require changes to business applications, systems or infrastructure, a change request is raised and associated with the incident / problem.

d) Incidents must be periodically analyzed to identify and act on structural problems.

5.2 IT Service Level Management

Control Objective
To implement and maintain the appropriate level of information security and service delivery in line with internal and third party service delivery agreements.

5.2.1 Service Level Agreements

Control
Service level agreements (SLA) exist with the internal and external service providers. The compliance to these agreements is regularly monitored.

Required Considerations

a) The SLA includes a clear description of the related services including security aspects and measurable levels of these services.

b) The SLA is up-to-date and signed by the involved parties.

c) Periodically, the SLA is evaluated to ensure it is aligned with the required service level of the end user organization.

5.3 Malicious Code and other threats

Control Objective
To protect the integrity of software and information against malicious code and other threats.

5.3.1 Malicious code

Control

Appropriate measures have been taken to prevent, detect and remove malicious code (e.g. ransomware, viruses, Trojan horses, worms).

Required Considerations

a) Intrusion detection must be implemented on perimeter and anti-virus software is installed on all servers and kept up-to-date. Anti-virus software is also installed on all workstations (laptops and desktops).

b) All software and data introduced to the network and workstation (e.g. through downloading or email) must be checked on malicious code before being used.

c) All workstations and servers must be regularly scanned for malicious code.

d) End-users must not be able to remove scanning software or interrupt scans.

e) Removal procedures exist and are followed when malicious code is detected.

5.5 Network Security

Control Objective
To ensure the protection on networks and the protection of the supporting infrastructure.

5.5.1 Network controls for LAN and WAN

Control

The access to the networks (both LAN and WAN) is adequately protected by security measures.

Required Considerations

a) Access control on the network is in place to ensure that only authorized devices can access the wide area network and local area network.

5.6 Electronic Exchange of Data

Control Objective
To maintain the security of information and software exchanged within the organization and with any external entity.

5.6.1 Electronic data exchange

Control

The confidentiality of information is ensured when exchanged within and outside the organization.

Required Considerations

a) Agreements with external parties must be established for the structural exchange of sensitive information and software between Grupo Promax and these parties (e.g. interfaces).

c) A user policy exists describing the security rules concerning the use of electronic communication and the use of Internet. This policy has been communicated to the organization.

d) Sensitive information must be protected before exchanged.

5.7 Detection of unauthorized activities

Control Objective To detect unauthorized information processing activities.

6 Access Control

6.1 Authorized User Access

Control Objective
To ensure authorized user access and to prevent unauthorized access to information, business applications and infrastructure.

6.1.1 Access control

Control
Access to information, business applications and infrastructure is restricted to authorized personnel only.

Required Considerations

a) Access control policy must be exists and is aligned with the business and security requirements for access. The rules and guidelines includes:
   - Security requirements per system,
   - Requirements for authorization of access requests,
   - Requirements for periodic review of access controls,
   - Removal of access right,
   - Password rules for IT components (e.g. business applications, operating system, database, network).

b) Access to information, business applications and infrastructure of users and support personnel is restricted in accordance with the defined access control policy.

c) A user registration procedure is in place for granting and revoking access to all IT components ensuring that each request is properly authorized and that access is revoked timely (e.g. at resignation and in case of an internal transfer).

d) The use of utility programs and special system privileges that might be capable of overriding system and application controls is restricted and tightly controlled.

6.1.3 Super user access

Control
User ID's with unlimited access to IT components must be properly managed (e.g. administrators, system users).

Required Considerations

a) The existence of these user ID's must be limited as much as possible.

b) These user ID's must be identified and the usage is approved by the IT Security Coordinator only after the reason for usage is well-founded.

c) User ID's with unlimited access must be not used by a group of people, but only by an identified person to guarantee the accountability.

d) Additional controls must be in place to manage the high risk related to these user ID's (e.g. logging the use of these user ID's and reviewing the data regularly).

6.2 Prevention of unauthorized user access

Control Objective
To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

6.3 Prevention of unauthorized network services

Control Objective
To prevent unauthorized access to networked services.

6.3.1 External network access

Control
All external network access connections must be appropriately secured and authorized.

Required Considerations`

a) All external network access connections must be registered and approved by IT department prior to implementation.
b) Appropriate authentication methods must be used to control access by remote users (employees, contractors and third parties), e.g. Virtual Private Networks with user and password.
c) Routing controls must be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications (e.g. by means of secure gateways).

7 Information systems acquisition, development and maintenance

7.1 Security as integral part of business applications

Control Objective To ensure that security is an integral part of business applications.

7.1.1 Attention for information security during development

Control
Information security is an integral part of the selection and development of business applications.

Required Considerations

a) Information Security is addressed in system development and changes in business applications.

b) IT Security Coordinator must be define security requirements for new business applications, or enhancements to existing business applications.

c) IT staff involved in the development of business applications implement security measures in accordance with the business requirements.

7.1.2 Acceptance testing

Control
Business representatives must be involved in acceptance testing before taking new business applications, upgrades, and new versions into the production environment.

Required Considerations

a) Acceptance criteria for new business applications, upgrades and new versions must be defined by business representatives before taken into production (including information security criteria).

b) Acceptance tests for business applications must be performed and authorized by business representatives before taken into production.

7.2 Confidentiality

Control Objective To protect the confidentiality of information.

7.2.1 Confidentiality of information

Control
Measures must be taken to secure electronically stored information that is highly confidential.

Required Considerations

a) The level of confidentiality for information (e.g. word, excel documents in folders) is determined.

b) Information that is classified as highly confidential is protected by additional security measures (e.g. encryption, passwords, and so on)

7.2.2 Protection of test data

Control
Sensitive production data used for (acceptance) testing outside the production environment is protected and controlled.

Required Considerations

a) When production data is used outside the production environment, this data is protected and controlled in a similar way as in the production environment.

7.3 Change Management

Control Objective
To ensure that changes in the production environment (business applications, systems and infrastructure) must be controlled.

7.3.1 Change Management – Authorization

Control
Only properly authorized change requests must be taken into development.

Required Considerations
a) Request for changes must be properly documented and administered. At least the following should be recorded:
- A description of the change;
- The urgency / priority of the change;
- The impact of the change, both within and outside the own Business Unit;
- The IT components related to the change.

b) Change requests must be formally authorized by the appropriate business representative after evaluation (e.g. costs vs. benefits, alignment with company polices).

7.3.2 Change Management - Testing

Control
All changes must be properly tested and approved before taken into production.

Required Considerations
a) Changes to business applications and systems must be tested by both the developers and appropriate business representatives.
b) Test results must be documented.
c) Approval must be obtained (based on the test results) before changes are migrated to the production environment
d) The system and infrastructure documentation is updated timely to reflect the changes made.

7.3.3 Change Management – Access restriction

Control
Access is adequately restricted to prevent direct changes being made to the production environment.

Required Considerations

a) System settings prevent system changes being made directly in the production environment.
b) Segregation of duties enforced by system access exists to ensure that the creation and modification of programs is not performed directly in the production, but in the development environment
c) Access to change production source code and customizing directly within the production environment must be controlled tightly. That means that access of developers to the production system is not allowed. Only in case of a disruption to business operations, developers are allowed into the production environment to solve problems under the condition that all activities of the development user id are logged and monitored afterwards.
d) Developers cannot migrate changes into the production environment themselves.
e) Access to transactions with which changes are moved into the production environment is highly restricted.

7.3.4 Change Management – Emergency changes

Control
Emergency changes must be implemented in a controlled manner.

Required Considerations

a) The emergency change procedure has been documented.
b) A clear definition must exist of emergency changes to ensure the procedure is only applied when necessary.
c) Emergency changes must be analyzed and authorized by a business representative once the emergency has been resolved.

8 Information Security Incident Management

Control Objective
To ensure information security events and weaknesses associated with business applications, systems and infrastructure must be communicated in a manner allowing timely corrective action to be taken.

8.1.1 Security Incidents – communication

Control
Security events and weaknesses must be detected and communicated in a manner that timely corrective action can be taken.

Required Considerations

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

b) Security events or suspected security weaknesses must be reported through appropriate management channels as quickly as possible.

c) Successful hacker attacks and significant virus attacks must be reported to the IT Manager.

10 Compliance

10.1 Compliance with any law, statutory, regulatory or contractual obligations

Control Objective
To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

10.1.1 Identification of applicable legislation

Control
All applicable legislation with respect to Information Security including IT must be identified by Legal department and where required measures must be taken by the Organization.

Required Considerations

a) All relevant statutory, regulatory and contractual requirements must be explicitly defined, documented, and kept up to date.
b) Depending of the legal requirements measures must be taken with respect to IT and information security.

10.1.2 Intellectual property rights (IPR)

Control
Guidelines must be considered to protect any material that may be considered intellectual property.

Required Considerations

a) Copyright of software must not be violated.
b) Only authorized software and licensed products can be installed on the IT infrastructure.
c) Checks must be must be carried out to verify that any maximum users permitted within a license is not exceeded (license management).

10.1.3 Data protection and privacy of personal information.

Control
Data protection and privacy of personal information must be ensured as required in relevant legislation and regulations.

Required Considerations

a) Data protection and privacy must be ensured within the IT environment as required in applicable legislation and regulations.
b) A data protection and privacy policy must be developed and implemented.
c) Technical and organizational measures to protect personal information must be implemented.

10.2 Sanctions for non-compliance Information Security Policy.

Control

Any breach regarding to this policy will be notified to the immediate manager, human resources or to whom it corresponds so that the pertinent measures will be taken.