ISITIX

Security Policy

Information Security Policy

Table of contents

1. Organizational security

1.1 Introduction

1.2 Roles and responsibilities

1.2.1 Information Security Officer
1.2.2 IT managers
1.2.3 Business representatives
1.2.4 Root domain access administrators
1.2.5 Employees
1.2.6 Board of Directors
1.2.7 Support functions

1.3 External entities

1.3.1 Clients
1.3.2 Suppliers and contractors

1.4 Security management process

1.4.1 Security Policy versioning
1.4.2 Security Policy publication
1.4.3 Security Policy enforcement
1.4.4 Delegation
1.4.5 Steering committee
1.4.6 Audit and control
1.4.7 Awareness improvement
1.4.8 Incidents management
1.4.9 Processes specific to external entities

2. Physical security of offices

2.1 Definition

2.2 Inventory of offices

2.3 Assessment of environmental risks

2.4 Workspace organization

2.5 Security of premises

2.5.1 Intrusion protection
2.5.2 CCTV
2.5.3 BMS
2.5.4 Fire safety systems

2.6 Security of office machine rooms

2.6.1 Physical access control
2.6.2 Energy
2.6.3 Cooling
2.6.4 Fire safety

2.7 Access control to the offices

2.7.1 Process and rules
2.7.2 Office closure

2.8 Accountability and auditability

3. Information security in the office workspace

3.1 Logical access control

3.1.1 User authentication service
3.1.2 Administrator authentication service
3.1.3 Workstation registration
3.1.4 User account management
3.1.5 User right management
3.1.6 Least privilege principle enforcement
3.1.7 Security strategy
3.1.8 Share directories and media servers

3.2 Network security

3.2.1 Zone isolation
3.2.2 Network device firmware update
3.2.3 Network device configuration management
3.2.4 Security against rogue stations
3.2.5 Internet flow control
3.2.6 Wifi

3.3 Workstation security

3.3.1 Inventory management
3.3.2 System security
3.3.3 Security patches and update management
3.3.4 Antivirus
3.3.5 Response to a suspected compromise
3.3.6 Security of network printers and peripherals
3.3.7 Security of message system and mail

3.4 Additional measures for mobile device (laptop, tablet, smartphone)

3.5 Accountability and auditability

3.6 Backup and restore

4. Security of computing resources

4.1 In-house server rooms

4.1.1 Responsibility
4.1.2 Location
4.1.3 Insurance policy
4.1.4 Access control
4.1.5 Energy
4.1.6 Cooling
4.1.7 Fire safety
4.1.8 Flood protection
4.1.9 HA, continuity and Disaster Recovery
4.1.10 Monitoring and logging

4.2 Security of outsourced datacenters

4.2.1 Service perimeter
4.2.2 Security policy, standard and certification
4.2.3 Legal, contractual and SLA
4.2.4 Control of external workforce, contractors and sub-contractors
4.2.5 Physical security, access control, intrusion protection
4.2.6 Environment, energy, cooling
4.2.7 Environmental risks protection
4.2.8 TelCo access
4.2.9 Hardware inventory management
4.2.10 Availability, SLA, Incidents management
4.2.11 Business continuity, crisis management
4.2.12 KPI
4.2.13 Auditability

4.3 Security of Infrastructure As A Service (IAAS)

4.4 Security of Software and Platform As a Service (SAAS and PAAS)

5. Servers and computing security

5.1 Security by design

5.1.1 Initial project
5.1.2 Evolutions

5.2 Update management

5.2.1 Assessing vulnerabilities

5.2.1.1 For key technical frameworks
5.2.1.2 For key assets

5.2.2 Vulnerability mitigation, update process
5.2.3 Zero-days management

5.3 Configuration management

5.3.1 Configuration building and testing
5.3.2 Configuration deployment
5.3.3 Configuration versioning

5.4 Isolation

5.4.1 Network isolation
5.4.2 Software defined (virtual environment) isolation

5.5 Authentication management

5.5.1 Inventory of authentication materials
5.5.2 Authentication materials (credentials, PKI, PGP keys…)
5.5.3 Protection of authentication materials
5.5.4 Production of authentication materials
5.5.5 Revocation
5.5.6 Logging of authentication activity
5.5.7 Auditability

5.6 Data protection policy

5.6.1 Data lifecycle management
5.6.2 Data event log management
5.6.3 Protection and ciphering
5.6.4 Backup management
5.6.5 Archives management

9. Glossary