INFORMATION SECURITY POLICY

Document No:
MPA-27001 POLICY

Rev:
B

Date:14.08.2015

***MilSOFT* Yazılım Teknolojileri A.Ş.**
Teknokent, 06800 ODTÜ Ankara

TÜRKİYE

1 Purpose

The purpose of this policy document is to establish management direction and high level objectives for ISMS.

2 References

- TS ISO/IEC 27001: 2013
- MilSOFT Security Handbook
- MPA-OMH ISO 9001 Quality Handbook

3 Structure of this Policy

This policy is based upon ISO 27002, ISO 27001 and is structured to include the 15 main security category areas within the standard.

This policy is a high level policy which is supplemented by information security processes which provide detailed procedures and guidelines relating to specific security controls.

4 Scope

This Information Security Policy outlines the framework for management of Information Security within the organization.

The Information Security Policy, standards, processes and procedures apply to all staff and employees of the organization, contractual third parties who have access to the organization's information systems or information.

The Information Security Policy applies to all forms of information including:

- speech, spoken face to face, or communicated by phone or radio,
- hard copy data printed or written on paper,
- information stored in manual filing systems,
- communications sent by post / courier, fax, electronic mail,

- stored and processed via servers, PC's, laptops, mobile phones, PDA's,

- stored on any type of removable media, CD’s, DVD’s, tape, USB memory sticks, digital cameras.

4.1 Terms and Definitions

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

4.1.1 Asset

Anything that has value to the organization

4.1.2 Control

Means of managing risk, including policies, procedures, guidelines, practices

4.1.3 Guideline

A description that clarifies what should be done and how

4.1.4 Information Security

Preservation of confidentiality, integrity and availability of information

4.1.5 Policy

Overall intention and direction as formally expressed by management

4.1.6 Risk

Combination of the probability of an event and its consequence

4.1.7 Third Party

Person or body that is recognized as being independent

4.1.8 Threat

Potential cause of an unwanted incident, which may result in harm to a system

4.1.9 Vulnerability

Weakness of an asset that can be exploited by one or more threats

External Interested Parties

1. Customers
2. Government Entities
3. ODTU Teknokent management
4. Suppliers
5. Media
6. Emergency services
7. Outsource Services

1- Customers

Before sharing an information with a potential customer an NDA shall be signed and all information exchange shall be arranged with respect to this agreement. In Contract awarding phase related security requirements shall be added to standard Terms and Conditions of Customer Contract.

2- Government Entities

Milsoft have facility Security Clearance issued by Ministry of Defence. This clearance shows that the facility is suitable for; storing classifed information, project or assets, and take necessary precautions has been taken to avoid internal and external threats, and comply with necessary rules of Ministry of Defence.

Physical, classification of information and information sharing are well defined in TÖGEK and ISMS system which is aligned with TÖGEK.

MilSOFT shall obey the laws like 3473 Law about archiving documents and material, 4857 Labor Law, 5070 Electronic signature Law, 6331 Occupational Health and safety, 5651 Regulating Broadcasting in the internet and Fighting Against Crimes Committed through Internet

Updates of these laws shall be tracked and related changes shall be adapted to MilSOFT processes.

3- ODTU Teknokent Management

Milsoft main facility is in the territory of ODTU Teknokent. Services like communication, electric, maintenance, transportation, water and natural gas are cooperated and aligned with ODTU Teknokent A.Ş.

4- Suppliers

Before sharing an information with a potential supplier an NDA shall be signed and all information exchange shall be arranged with respect to this agreement. In Contract awarding phase related security requirements shall be added to standard Terms and Conditions of Subcontract/Purchase Order.

Before sharing an information with partners and suppliers a NDA shall be signed and all information exchange shall be arranged with respect to this agreement.

5- Media

For publishing information from internet there are two sources which are internet website and social accounts. These sources shall be managed with respect to MPA-CS-Pd22 External Account Management procedure.

6- Emergency Services

In ISMS system related emergency services are defined in TÖGEK. Point of Contact information are provided in TÖGEK.

7- Outsource Services

Outsource service contracts are managed by Administrator Affairs Manager like cleaning and outside security. A written contract is taken from every worker who is working in Milsoft for supporting purposes. In these documents all the security concerns and regulations are explained to the worker and signature is taken.

Internal Interested Parties

1. Employees
2. Top Management

1- Employees

In the Staffing procedure for new employees, a number of tests, validations, written contracts, and training are made with respect to the MPA-HR-Pc03 Staffing Process and Information security concerns are part of this process. In parallel to these requirements, every year Information Security Awareness trainings for all employees are performed for ISMS system.

2- Top Management

ISMS system is supported by top management. Documents like as ISMS Policy, Risk Assessment and Treatment Plan, Information Security Continuity Plan, Recovery Management Strategy Matrix are reviewed and approved by Directors, Vice Presidents and General Manager in case of change. Once a year ISMS system review meeting is held with Directors, Vice Presidents, and General Manager.

Above interested parties' inputs are used for the determination of ISMS scope. Control objectives and controls that shall be used in this ISMS scope are given in related sections of ISMS Policy document. Details of these controls and additional actions shall be maintained in accordance with Risk Management for Information Technologies process.

5 Management Responsibility

Information is an asset that the organization has a duty and responsibility to protect. The availability of complete and accurate information is essential to the organization functioning in an efficient manner and to providing products and services to customers.

The organization holds and processes confidential and personal information on private individuals, employees, partners and suppliers and information relating to its own operations. In processing information, the organization has a responsibility to safeguard information and prevent its misuse.

The Information Security Policy is a high-level document, and adopts a number of controls to protect information. The controls shall be delivered by policies, standards, processes, procedures, supported by training and tools.

The Information Security Policy shall be approved by management, and set out the organization's approach to managing its information security objectives.

The Information Security Policy shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

All information security responsibilities shall be defined and allocated.

Information security implications shall be analyzed, addressed and reviewed regularly in all projects.

6 Higher Level ISMS Policies

In the scope of TS ISO/IEC 27001 Information Security Management Systems standard, our policy is to:

- Comply with all TS ISO/IEC 27001 requirements and all related regulations,
- Continuously improve information security management system,
- Provide integrity, protect privacy and usability of company and customer assets,
- Maintain business continuity.

This information policy document will be communicated with related MilSOFT personnel during ISO 27001 ISMS training courses. Policy document will be maintained and will available to all related MilSOFT personnel and to the interested parties.

6.1 Objectives

The ISMS framework that is derived from above mentioned policies provides the following objectives;

- To provide access of information only to authorized persons from within or outside the company,
- To maintain confidentiality of information,
- To train all related personnel on information security,
- To report and investigate all incidents for information security.

Quantitative objectives that are defined by higher level management are documented and maintained in Organizational Measurement Plan (OMP).

7 Lower level ISMS Policies

Derived lower level detailed policies as follows:

7.1 Stakeholder Engagement

The Information Security Policy shall be communicated to employees and relevant external parties.

Procedures for appropriate contacts with relevant authorities shall be in place and maintained accordingly.

Procedures for appropriate contacts with special interest groups or other specialist security forums and professional associations shall be in place and maintained accordingly.

7.2 Human Resource Security

All candidates shall provide a legal background check provided by Attorney General, and after their employment application for “National Secret” level clearance will be made to Ministry of National Defense for additional screening.

The screening requirements shall also apply to contractors.

The contractual agreements with employees and contractors shall state their and organization’s responsibilities for information security.

Management shall ensure that all employees and contractors shall be aware and work in line with company Information Security regulations.

Management shall ensure that all employees and the relevant contractors shall receive appropriate up to date awareness education and training.

A formal and communicated disciplinary process shall be applied to those employees who have committed an information security breach.

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

7.3 Asset Management

7.3.1 Responsibility for Assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be established and maintained.

Each asset maintained in the inventory shall have an owner.

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

Employees and external party users using or having access to the organization’s assets shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

7.3.2 Information Classification & Handling

Information shall be classified according to rules set by MilSOFT Security Handbook which is compliant to Ministry of Defense Facility Clearance regulations, in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

Information labeling shall be done in accordance with the information classification scheme adopted by the organization. Procedures for information labeling shall cover information and its related assets in physical and electronic formats.

Handling of assets shall be done in accordance with the information classification scheme adopted by the organization.

7.3.3 Media Handling

Removable media shall be managed in accordance with the classification scheme adopted by the organization.

Media shall be disposed of securely when no longer required, using formal procedures.

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

7.4 Access Control

7.4.1 Business Requirement for Access Control

Appropriate access control rules, access rights and restrictions shall be established, documented and reviewed based on business and information security requirements.

Critical information is documented on Information Access Rights Map (I-ARM). Any change to I-ARM shall be subject to the approval of the Board of Directors (see Annex A).

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

7.4.2 User Access Management

Formal user registration and de-registration shall be implemented to enable assignment of access rights.

Formal user access provisioning shall be implemented to assign or revoke access rights for all user types to all systems and services.

The allocation and use of privileged access rights shall be restricted and controlled.

The allocation of secret authentication information shall be controlled.

Asset owners shall review users’ access rights at regular intervals.

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

7.4.3 User Responsibilities

Users shall be required to follow the organization’s practices in the use of secret authentication information.

7.4.4 System and Application access control

Access to information and application system functions shall be restricted.

Access to systems and applications shall be controlled by a secure log-on procedure when required.

Password management systems shall be interactive and shall ensure quality passwords.

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

Access to program source codes shall be restricted and shall be under control of Configuration Management Department.

Conflicting duties and areas of responsibility shall be segregated so that no single person access, modify or use assets without authorization or detection. (6.1.2)

When using mobile devices, special care shall be taken to ensure that business information is not compromised. (6.2.1)

Employees can use their private mobile devices in the work environment, but they can not access to business information. (6.2.1)

Teleworking activities are not allowed by MilSOFT. (6.2.2)

7.5 Cryptographic Controls

The principles on the use of cryptographic controls for protection of information shall be developed and implemented.

Use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

7.6 Physical and Environmental Security

7.6.1 Secure Areas

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities as defined in MilSOFT Security Handbook.

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access as defined in MilSOFT Security Handbook.

Physical security for offices, rooms and facilities shall be designed and applied as defined in MilSOFT Security Handbook.

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied as defined in MilSOFT Security Handbook.

Procedures for working in secure areas shall be done according to MilSOFT Security Handbook.

Administrative offices where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

7.7 Equipment

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

Equipment shall be correctly maintained to ensure its continued availability and integrity.

Equipment, information or software shall not be taken off-site without prior authorization.

Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Users shall ensure that unattended equipment has appropriate protection.

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

7.8 Operations Security

7.8.1 Operation Procedures and Responsibilities

Operating procedures shall be documented and made available to all users who need them.

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

7.8.2 Protection from Malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Protection against malware shall be based on malware detection and repair software, information security awareness and appropriate system access and change management controls.

7.8.3 Backups

Backup copies of information, software and system images shall be taken and tested regularly.

The number of backup copies, number of locations to store backups, and responsible personnel are subject to the approval of the Board of Directors (see Annex B).

7.8.4 Logging and Monitoring

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

Logging facilities and log information shall be protected against tampering and unauthorized access.

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

7.8.5 Control of Operational Software

Installation of software on operational systems shall be controlled.

7.8.6 Management of Technical Vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Rules governing the installation of software by users shall be established and implemented.

7.8.7 Information Systems Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

7.9 Communications Security

7.9.1 Network Security Management

Networks shall be managed and controlled to protect information in systems and applications.

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

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

Unauthorized devices cannot be connected to the company network; necessary precautions shall be taken to prevent any occurrences.

Any device that is connected to the company network cannot exit the company premises without passing through a sanitization process. Only after the approval of the information security personnel that the device do not include any recoverable data, then it may be permissible to take the device out.

7.9.2 Information Transfer

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements shall address the secure transfer of business information between the organization and external parties.

Information involved in electronic messaging shall be appropriately protected.

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

7.10 System Acquisition, Development and Maintenance

7.10.1 Security Requirement of information systems

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

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

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

7.10.2 Security in development and support processes

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

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

If there is no contractual commitment, Executive Board approval is required for all types of source code release to out of company.

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Secure development environments for system development and integration efforts that cover the entire system development lifecycle shall be established and appropriately protected.

The organization shall supervise and monitor the activity of outsourced system development.

Testing of security functionality shall be carried out during development.

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

7.10.3 Test Data

Test data shall be selected carefully, protected and controlled.

7.11 Supplier Relationships

7.11.1 Information security in supplier relationships

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

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

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

7.11.2 Supplier service delivery management

Organizations shall regularly monitor, review and audit supplier service delivery.

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

7.12 Information security incident management

7.12.1 Management of information security incidents and improvements

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

Information security events shall be reported through appropriate management channels as quickly as possible.

Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

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

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

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

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

7.13 Information Security Aspects of Business Continuity Management

7.13.1 Information security continuity

The information security requirements shall be determined and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

Appropriate processes, procedures and controls shall be established, documented, implemented and maintained to ensure the required level of continuity for information security during an adverse situation.

The established and implemented information security continuity controls shall be verified at regular intervals in order to ensure that they are valid and effective during adverse situations.

7.13.2 Redundancies

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

7.14 Compliance

7.14.1 Compliance with legal and contractual requirements

All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

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.

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatorylegislatorylegislation, regulatory, contractual and business requirements.

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. Milsoft works complaintcomplaintin accordance with labor law 4857 and health and safety law 63301.

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

7.14.2 Intellectual property rights

Intellectual property regulations in MİLSOFT and protect MİLSOFT products are managed by Intellectual Property Compliance Policy.

Approach to managing information security and its implementation shall be reviewed independently at planned intervals or when significant changes occur.

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.

Annex A: Information Access Rights Map (I-ARM)

Information	**Owner of Information**	**Authorized Personnel for Access**
Information Systems Access Rights	Information Systems	Assigned Information Systems personnel
Configuration Management Master Library	Configuration Management	Configuration Management team
Configuration Management archieve	Configuration Management	Configuration Management Manager
Backups	Computer Services	Computer Services Manager
Department Common Storage Area (Z:/ Drive)	Creator Department	Personnel approved by Creator Department's Manager
Project Common Storage Area (Z:/ Drive)	Creator Project	Higher level Managers in hierarchical order and personnel approved by Creator Project's Manager
Product Line Common Storage Area (Z:/ Drive)	Creator PL	Higher level Managers in hierarchical order and personnel approved by Creator Product Line's Manager
Finance Records (Z:/ Drive)	Financial Affairs Directorate	Financial Affairs Directorate
Yönetim Kurulu Raporları	Financial Affairs Directorate	Board of Directors, Financial Affairs Personnel
Teklif Fiyatlandırma Verisi	Financial Affairs Directorate	Finance Manager, Proposal Manager, VP Programs & Contracts, Acquisition and Contracts Director
Konsolide Bütçe	Financial Affairs Directorate	Board of Directors, Assigned Financial Affairs Personnel
Mali Tablolar	Financial Affairs Directorate	Board of Directors, Financial Affairs Personnel
Strategic Business Plan	Business Development & Marketing	Board of Directors, General Manager, Vice-Presidents, Department Directors, Functional Managers

Measurement Repository	Quality Management	Assigned QM personnel
Processes/Procedures (in word format)	Quality Management	Assigned QM personnel
Personnel Performance Evaluation Files	Human Resources	HR Manager, HR Specialist, Higher level Managers of the personnel in hierarchical order
Personnel File	Human Resources	İK Yöneticisi, İK Uzmanı
Salary/Payroll Data	Human Resources - Personnel	Financial Affairs Director, Assigned Financial Affairs Personnel, HR Manager
Personnel Contracts	Human Resources	HR Manager
Payment and Letter of Credit Data (Ongoing Projects)	Acquisition and Contracts	VP Contracts and Programs, Acquisition and Contracts Director, Contract Manager, Contract Specialist
Personnel Security Clearences	Administrative Affairs & Security	Administrative Affairs & Security Personnel
Physical Access Records	Administrative Affairs & Security	Administrative Affairs & Security Manager
Signed versions of: -Customer Contracts - Subcontracts / Payment Agreements under each customer contracts -Side Agreements and other documents of legal/contractual importance under such customer contracts -Any ammendment(s) thereto	Acquisition and Contracts	VP Acquisition, Contracts and Programs, Acquisition and Contracts Director
Signed versions of Agreements for business development purposes; - MoU(s) - NDA(s) - Teaming Agreements	Acquisition and Contracts	VP Acquisition, Contracts and Programs, Acquisition and Contracts Director, Marketing and Business Development Director

- Cooperation Protocols - Any ammendment(s) thereto		

Annex B: Backup

Backup Info	**Number of backup copies**	**Locations**	**Responsible personnel**
Project data (source code, document, design, requirements, etc.)	1 disc 1 disc 1 cartridge	System room in server (Ankara) System room in server (Istanbul) System room in safe box (Ankara)	Computer Services Manager
Shared workspace (Z:/)	1 disc 1 disc 1 cartridge	System room in server (Ankara) System room in server (Istanbul) System room in safe box (Ankara)	Computer Services Manager
Server configurations	1 disc 1 disc	System room in server (Ankara) System room in server (Istanbul)	Computer Services Manager