FYEO INC		Internal INSTRUCTION	1 (31)
Prepared by (also subject responsible if other) Thomas Olofsson/James Selby		No. 1	Rev 2015-03-15
Doc responsible/Approved	Checked	Date 26/3/23	File C:\Security
Document title FYEO Limited ISMS			

FYEO INC
Security Management System
Policy

1 CISO Statement

Security measures are prudent housekeeping. There is always a balance to be struck between over indulgence in security matters and being too lax. Over indulgence can inhibit the operational running of the business and be expensive: lack of security can have disastrous consequences.

This document sets out the FYEO Company Security Policy. This Policy is to be understood and applied by all employees (including temporary), contractors and consultants. This document itself is confidential to the company and should if printed be retained in a safe place. Reference will be made to this policy in the contract of employment signed by employees.

Underpinning the Company Security Policy will be a number of specific security procedures and security initiatives running across FYEO. Nothing is designed to replace the common sense, sound judgment and discretion of employees, contractors and consultants. But this Policy is a statement of the company's commitment to establishing and maintaining good security practices. This can only benefit FYEO Limited and in turn its employees and customer relationships.

Please ensure you give the Company Security Policy, and all security measures, your full support.

Thomas Olofsson
CTO / CISO
FYEO INC

Scope and purpose of the Security Policy

The Security Policy aims to support all employees at FYEO Limited and to increase their awareness in the areas of Information Security.

1.1 FYEO Limited Information Security Management System Policy statement

All employees, consultants and subcontractors have a fundamental responsibility to safeguard and protect company assets against loss or damage, no matter what the cause, and to co-operate with the company in the implementation and maintenance of good security practices.

1.1.1 Scope

The Security Policy applies to all aspects of company operations and business and cover FYEO's products and services at all stages, facilities, sites and workplace in general. It applies to all business processes and projects, systems and networks, internal communication and to communication with external organizations, contractors and customers.

The policy document is approved by management and published and communicated, as appropriate, to all employees. It states management commitment and set out the organization's approach to manage information security.

Security must be addressed at all stages of business processes, products and services

1.1.2 Purpose

The Security Policy acts as guidelines to all employees of Xxx and have been created to support employees in their daily work and to enhance the information security awareness of the company and all its employees.

1.1.3 Definition

Information security is defined as the preservation of confidentiality, integrity and availability of information.

- Confidentiality – ensuring that information is accessible only to those authorized to have access
- Integrity – safeguarding the accuracy and completeness of information and processing methods
- Availability – ensuring that authorized users have access to information and associated assets when required

2 Organizational security

All employees are responsible to keep a good level of security at FYEO, however greater responsibility lies with the Security working group and with managers to make sure employees are updated against routines and guidelines.

2.1 Information security infrastructure

A management framework for information security infrastructure must be clearly defined and implemented to manage information security within FYEO.

2.1.1 Security department

The Security Department shall support the Head of Security, and the members of the department shall support the organizational managers and cooperatives in security matters. All employees must be informed about the responsibilities of the Security Department and how to contact the group.

Tasks of the Security Department includes the following:

- General
    - Participate in the development of security functions within FYEO Limited
    - Assessment of information security and be able to take action when needed
    - Participate in the development of physical security routines
- Act as a point of contact
    - Maintain contact between different departments in a security interest
    - Maintain contact with outside organizations in a security interest
- Fire and Escape
    - Inform employees of company routines regarding escape during emergencies
- Unauthorized persons
    - Taking actions against unauthorized persons in accordance with own judgment
    - Report to the Head of Security or the nearest manager
- Information security
    - Master and understand regulations regarding information security
    - Support managers and cooperatives within own department or unit
    - Report incidents, etc. to the Head of Security
- Education
    - Continually educate and inform employees regarding Xxx security standards

2.2 Allocation of information security responsibilities

Different roles are defined to state responsibility within FYEO organizations for information security according to the following.

2.2.1 General responsibilities

Final responsibility within FYEO Limited lies with the line management, however each individual is personally responsible and accountable for the security of his or her operations and actions within FYEO Limited.

2.2.2 Security Responsible

- Responsible for developing guidelines, routines and the information classification model
- Responsible for informing about security to new employees within FYEO Limited
- Responsible for signing a non-disclosure agreement with new employees and to account for meaning of this agreement
- Responsible for that new employees are educated and trained about security at the first opportunity of education

2.2.3 Information owner

- Keeping models of classification updated to the business
- Inform about changes regarding the information classification
- Audit and follow-up the adherence of FYEO classification model

2.2.4 Individuals

- Responsible that information is classified in accordance with FYEO information classification model
- Responsible that only authorized persons are getting access to information and thereby preventing the disclosure to unauthorized persons
- Responsible for deciding who is authorized, otherwise this is decided by the nearest manager.

2.2.5 Employees purchasing services or products

- Responsible that signing of non-disclosure agreements by consultants, contractors etc. are done

2.2.6 PC-operation

- Responsible that distribution and transport of computers and storage medias that are to be repaired or destructed is treated according to FYEO Limited regulations and instructions.

3 Personnel security

Employees are not expected to put themselves at any physical risk in the course of their work or on behalf of the company. Management is responsible to inform all employees of their responsibilities regarding security.

3.1 Security in job definition

Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment in order to reduce the risks of human error, theft, fraud or misuse.

3.1.1 Employment contract

Terms of employment must withhold information about the employees' responsibility regarding information security. These responsibilities must continue for a defined period after the end of employment, which should be stated on the employee contract.

Legal responsibilities and rights should be clarified and included within the terms and conditions of employment.

Reference to this policy will be made in the contract of employment.

3.1.2 Confidentiality agreement

Confidentiality or non-disclosure agreements are used to give notice that information is confidential or secret. Employees must, in relation to their time of employment, sign a non-disclosure agreement as part of their terms of employment.

3.1.3 Termination of employment

When an employment is terminated, the following measures must be performed:

- Recover all FYEO property, such as ID cards, laptops, mobile phones, dongles, printed material, intranet access and other information.
- Ensure that all access to systems, networks and applications are revoked prior to departure. An exit form should be initiated by Human Resources and sent to responsible security administrators to complete the termination of employment.
- Ensure that staff is aware of the signification of the signed non-disclosure agreement and its expiration time.

3.2 Responding to security incidents and malfunctions

Responsibilities and routines regarding incident handling must be stated to ensure quick, effective and routinely reactions when security incidents occur. These routines must be introduced to all employees and placed on FYEO intranet where all employees have access to them.

3.2.1 Reporting security incidents and weaknesses

A formal reporting procedure should be established and introduced to all employees and contractors, to be used for reporting security incidents and weaknesses as quickly as possible.

Employees are obligated to report any incidents, including theft, damage, fraud, disclosure of information, network or IT misuse, which is defined as behavior that could be damaging for FYEO Limited. Proper software must be installed on desktops, laptops and other system to monitor and report software malfunctions and viruses.

All staff must report any incidents and breaches of this policy to their line manager. A comprehensive note should be made detailing:

- Suspected incident
- Time of observation
- Loss or effect on business
- Suspected persons involved and/or witnesses

The line manager is to forward this to the Security working group on email address **security@gofyeo.com**

3.2.2 Disciplinary process

A formal disciplinary process for employees who have violated FYEO's security policies and procedures should exist to ensure correct treatment for employees who are suspected of breaches of security and to act as a deterrent to employees inclined to disregard security procedures.

3.3 Mobile work and telecommuting

Information security must be maintained when using mobile equipment and during telecommuting by working in accordance with a formal policy and suitable instruments of control to protect against the risks with the usage of mobile equipment, especially in unprotected environments. Fyeo is a remote first company and therefore the policies and procedure for remote work is very important.

3.3.1 Mobile computing

When using mobile equipment of any kind, special care must be taken to protect FYEO information from being compromised. A formal policy must be adapted that includes access controls, cryptographic techniques, back-ups and virus protection.

3.3.2 Telecommuting

Suitable protection of the telecommuting site should be in place to reduce the risk of unauthorized remote access to FYEO's internal systems.

3.4 User education

Head of Security shall see to that:

- Employees at their occasion of employment are given information about security and signing of a non-disclosure agreement at FYEO Limited.
- Employees are given a security education, which is conducted during the first educational opportunity.

Training and education must ensure that users are aware of threats and risks regarding information security in a way that they are well prepared in their daily work to support FYEO's information security policy.

When relevant, third-party users should receive the proper training and updates to FYEO's policies and procedures, including security requirements and legal procedures.

4 Physical and environmental security

These regulations aim to prevent unauthorized access, damages and disturbances in the facilities of the FYEO organization and its information and also to prevent losses, damages or effects to assets and disruptions in the business.

4.1 Secure areas and compartments

The facilities of FYEO must be strictly controlled and only authorized personnel may be located within the facilities. Since FYEO is a remote first company this section applies mostly to server areas and colocation areas. All employees have the responsibility to ensure these restrictions. When working from home it is important to protect any data and data holding devices from unauthorized use.

4.1.1 Access control

Secure areas and compartments within FYEO must be protected by the use of suitable access controls, so that only authorized persons can gain access to these areas.

Physical security is achieved by establishing physical barriers around business premises and information processing facilities, and limiting access to authorized personnel. Card controlled entries are used to maintain the physical barriers on FYEO premises.

Employees possess an electronic ID card that is used to access the facilities, the card and is personal and must be kept confidential.

Loss of the ID card must be immediately reported.

4.1.2 Protecting offices, rooms and facilities (no requirement at this time)

Protected areas must be developed to protect offices, rooms and resources that are comprised by special security requirements. Areas such as NOC and Security Offices have restricted access.

The Security department is responsible for the physical security of the office buildings.

4.1.3 Visitors (No requirements at this time)

Visitors to FYEO facilities in Stockholm must be announced at the front desk and must be accompanied at all times by the employee receiving the visitor. Visitors may not be left alone in FYEO facilities.

4.2 Computer equipment security

Equipment belonging to FYEO must be located and protected in a secure manner to reduce the risk of environmental threats, dangers and opportunities for unauthorized access. Security routines must also be introduced so that equipment located outside the organization’s premises is secure.

4.2.1 Equipment inventory

An inventory list must be maintained and updated by the facility management at FYEO and a copy of the inventory list must be stored off-site/secure Intranet.

4.2.2 Equipment disposal

Equipment, information, data and software that belong to the organization must not be disposed of without approval. All equipment containing storage media must be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal.

4.2.3 Power supply

Equipment should be protected from power failures by a suitable electrical supply with multiple feeds to avoid a single point of failure in the power supply.

4.2.4 Cabling security

Power and telecommunication cabling should be protected from interception or damage. When possible, cabling should be placed under ground and power cables and communication cables should be segregated to prevent interference.

4.2.5 Equipment off-premises

The security provided should be equivalent to that for on-site equipment and includes all forms of personal computers, organizers, mobile phones, paper or other form. Employees are responsible for the security of equipment brought outside Xxx facilities.

4.3 Clear desk and clear screen policy

The FYEO organization adopts a clear desk and clear screen policy to avoid unauthorized access, loss of, and damage to information during and outside normal working hours. The clear desk and clear screen policy takes into account the information classification system adopted by FYEO stated in this policy document.

This includes logging out of, or locking of all computers when leaving them unattended.

5 Operations management

Security must be an integrated part of the operations and procedures of all departments of FYEO Limited and security awareness shall be integrated in all projects.

5.1 Procedures and responsibilities

Operating procedures must be formally documented and management must authorize any changes.

Operating procedures should be defined for each project within FYEO and those procedures should specify detailed instructions for execution of each job; this should include handling of information, scheduling requirements and instructions for handling errors or other exceptional conditions.

Within each project and operation, roles and responsibilities should be clearly defined that states who is responsible for taking the appropriate security considerations.

Deployment, installation, operation and recovery procedures of IT systems, applications and network services must be planned, tested and documented. Risk assessment of new systems is mandatory before deployment.

5.1.1 Operational change management

Changes to information processing facilities and systems must be managed and coordinated by management in order to prevent system or security failures. Audit logs should be retained and should contain all relevant information.

5.1.2 Incident management

All employees must report system and security incidents to their closest manager or to the Security working group as soon as they are discovered. This includes possible attacks and viruses as well as system failures and denial of service or other errors.

5.1.3 Separation of development and operational facilities

A level of separation between development, test and operational environments must be maintained to prevent operational problems and to prevent the introduction of untested code into operational environments.

Patches, updates and new software must be fully tested in isolated environments before being introduced in operational environments. No testing should be performed in operational environments.

Each business or development project is responsible for the complete testing of new software and systems before handing them over internal IT for deployment in the operational environments.

5.1.4 Backups and logs

All software and user data in the production environment will be backed up to alternative media on a regular basis and kept in a secure area. The backups will be used to completely restore the systems in case of a critical failure.

Changed system files will be backed up on a daily bases and a periodic full backup of all system files will be taken to provide baseline data integrity.

6 Information security

All information concerning FYEO that is externally distributed, will affect customers view on the company and our trademark. The routines within FYEO regarding classification and the protection of information, aims to prevent company internal or confidential information being disclosed to unauthorized persons.

6.1 Information classification

All information created, stored, processed, transmitted or printed by or on behalf of FYEO is the property of FYEO Limited, this information is an asset of FYEO and all staff are personally responsible for safeguarding the integrity and confidentiality of that information.

6.1.1 Classification of information

Classification of information must be done in accordance with the following statements that indicates the need and degree of protection:

Open information – No harm is done if the information is disclosed to unauthorized persons. Includes information produced for customers, i.e. commercial campaigns, presentations and product offers.

Internal information – Can cause harm to FYEO if the information is disclosed to unauthorized persons. Includes information of value to FYEO and which is produced for the company needs, i.e. organizational plans, system catalogues, employee records, on-going projects, customer agreements and internal information.

Confidential information – Can cause serious harm to FYEO if the information is disclosed to unauthorized persons. Includes information that may not be distributed outside the company, i.e. prognoses, calculations, budget propositions, market plans, blueprints, patents, product records, records of employment wages, employee matters and security systems.

E-commerce information – Applications and information regarding E-commerce should be PCI compliant and in general be closely monitored in such a way that outside threats can be avoided. It is the responsibility of each department manager to make sure that necessary actions are taken to secure this.

Internal and confidential information are represented as classified information.

6.1.2 Handling of internal and confidential information

For a closer description of FYEO’s guidelines regarding the handling of confidential information, please see further information about information classifications below. FYEO Limited document templates must be used when producing documents.

6.1.3 Guidelines for information classification

General – All information about Xxx that is externally distributed will affect the customers view regarding the company and our trademark. Coordinated and correct information will emphasize the trademark and the FYEO Company. The intention for routines regarding classification and the proper protection of information is to prevent company internal or confidential information being disclosed to unauthorized persons.

Responsibility – The Head of Security is responsible for guidelines, routines and audits regarding information classification.

The creator or receiver of information is responsible for:

- The proper classification of that information
- The distribution of that information to the right persons
- Deciding who is primarily authorized to access the information

Regulations

Verbally given information – Those who verbally distribute classified information shall inform the receivers that the information is classified, either as internal or confidential.

Mail and conveyance – Classified data or information must be distributed in such a way that disclosure of contents by unauthorized persons is prevented. Internal e-mail may be used for all kinds of information. However, confidential information distributed as internal e-mail must be limited. Confidential information that must be distributed externally, e.g. by the Internet, must be distributed in an encrypted way.

6.1.3.1 In other respects

Travelling – When traveling with classified documentation, confidential information must always be under supervision or kept locked away in a secure manner. Laptops with confidential information must be encrypted and documents may not be left on any premises.

Production of documents – Documents containing confidential information must be produced in a limited way and must be marked with “confidential” or “internal” in the document header in accordance to FYEO templates for internal documents. CD’s, USB’s and other sort of medias must also be marked if they contain classified information. When printing confidential documents, the documents may not be left unattended by the employee printing them.

Copying and destruction – Copying and destruction of confidential documents should be done by the issuer.

Storage – Confidential documents should be kept in locked areas and further, may not be kept on office desks during longer meetings or pauses.

Portable media – Confidential documents must be encrypted when stored on portable media like USB disks, portable hard disks, MP3 players etc.

Customer information security

All employees handling customer information must be informed of confidentiality regulations regarding information about customer’s personal data and subscription data at the time of employment.

Information about customer’s personal data and subscription data may only be revealed to the subscription holder.

Any unauthorized compilation, processing or release of customer information may be a legal offense against the Personal Data Act (GDPR) and would be a serious breach of customer confidentiality and it would be classed as professional misconduct.

The conditions whereby release of certain information to law enforcement agencies can take place are strictly controlled and can only be performed by dedicated staff. Any requests for information, such as identity of subscribers etc. must be communicated to the Security working group.

7 Access control and network security

All information access must be managed on a “need-to-know” basis, i.e. only information that is necessary for solving decided duties or specific tasks in accordance with the job description shall be available to individual users.

7.1 Authorization and access control

Organization requirements regarding access control must be defined and documented and access must be limited in accordance with the access control policy, which is based on the principle of least privilege.

7.1.1 Control of user access

A formal procedure shall control all stages in the life cycle of user access, from initial registration of users to final de-registration of users.

Username and passwords are used to prevent unauthorized access to information systems. Usernames must be unique so that users can be linked to and made responsible for their actions.

Periodical checks for redundant user ID’s and accounts must be performed and if found, redundant ID’s must be removed.

Users are claimed to ensure that unmanned equipment (desktops and laptops) are properly protected and locked when left unattended. When sessions are finished they must be terminated.

7.1.2 User password management

Users are claimed to choose and use good passwords, for the good of security, and further prompted to change their passwords on a regular basis. Passwords must not be shorter than 6 (six) characters in length.

Users must be informed to keep personal passwords confidential and work group passwords solely within the members of the group. User passwords may not be stored in an unprotected form.

7.1.3 Administration privileges

Administrator privileges must be granted on a very restrictive basis to end users to avoid misuse of systems.

7.1.4 Network management

Instruments of control and monitoring must be introduced to protect information and to obtain and maintain security in the network and in its additional infrastructure.

Users must only have direct access to those services that they specifically have authorization to use. For external connections, users must be authenticated through strong authentication techniques, e.g. virtual private networks or similar.

Proper documentation of the network of FYEO must be established in order to maintain the security of the network. These documents are regarded as confidential information and should be protected as such.

Sensitive systems must be handled in dedicated, i.e. isolated environments. Applications containing critical or classified information must be separated from other applications. Dedicated technical platforms should be considered for sensitive or critical systems.

Inactive computers will time-out after 15 minutes, clear the screen and require the user to re-authenticate before access is granted.

7.1.5 User authentication for external connections

Access by remote users should be subject to proper and strong authentication, using cryptographic techniques and hardware tokens (two factor authentication).

The number of unsuccessful access attempts should be limited and logs must be kept to follow up possible attacks.

7.1.6 Monitoring

Audit trails for divergence and other security relevant events must be registered and maintained for an agreed period of time to ease future forensics and to audit the access control system. Routines for regular supervision of information handling resources must be introduced and the result of this supervision must regularly be audited.

Monitoring logs of system use should be kept in order to ensure that users only are performing activities they are authorized for. Management and security personnel will have the opportunity to view these logs in case of suspicion of misuse.

7.2 Malicious software

To maintain the integrity of software and information, detection and protection against malicious software must be introduced, as well as suitable routines that help making the users aware of these problems.

7.2.1 Controls against malicious software

Back up of important business information and software must be done on a regularly basis. Operating staff must log their work.

Anti-virus software must be installed on all computers and media and kept updated on a regularly basis. All files including email attachments obtained from external resources must be checked against malicious software. Email attachments from unknown senders must not be opened.

If employees suspect a virus or other malicious software they must immediately report this to the appropriate personnel.

8 Communication security

Special security actions shall be considered to protect information belonging to Xxx in transmission, both within the company and to external partners, contractors and organizations.

8.1 Exchange of information and software

Agreements regarding electronic or manual exchange of information and software between organizations must be stated to prevent losses, changes and misuse of information that is being exchanged.

8.1.1 Media security during transportation

Media must be protected against unauthorized access, misuse or distortion during transportation.

8.1.2 Electronic commerce security

Electronic commerce must be protected against fraudulent proceedings, violation of agreements and disclosure or alteration.

8.1.3 Email security

FYEO Limited reserve the right to access and disclose all messages sent over its email system, for any purpose. Employees may use company email for personal communication but must be informed that all email sent over Treat Finder systems are the property of FYEO Limited.

Internal mail may not be forwarded to addresses outside the FYEO organization.

Internal or Confidential information must be encrypted when sent to addresses outside FYEO Limited.

8.1.4 Internet and other public networks

Internet and other public networks are not considered to be secure and users must exercise good judgement in using these networks. Users are responsible for the reliability of sites used for research or software downloading.

Third-party security

The security of the FYEO organizations information handling resources and information assets must be maintained during third party access.

8.1.5 Third-party risk analysis

Risks regarding third party access to the organizations information handling resources must be assessed and applicable precautions and assessments taken.

Third party access to FYEO’s information and handling resources must be based on a formal agreement that includes all necessary security requirements.

8.2 Outsourcing

Information security must be maintained when the responsibility for information handling has been outsourced to an external organization. When outsourcing is used, risks, routines and actions taken regarding security for information systems, networks and/or personal computers, must be taken into consideration in a mutual agreement (contract) between parties.

Contracts between FYEO and outsourcing organizations must specify legal requirements, security responsibilities and information access.

9 Systems development and maintenance security

Security awareness in development and maintenance processes is vital to ensure the integrity of data and to avoid errors that may have an impact on company information security.

9.1 System planning

All systems used within FYEO must be set up and distributed in ways that minimize the risk of system failures. Security requirements must be defined and included in all FYEO business projects prior to the development of systems, applications and networks.

9.1.1 Risk assessment

A risk assessment is to be carried out before each phase of the development where technical and procedural threats and potential damage are analyzed. Appropriate controls for prevention of confidentiality, integrity and availability loss, as well for logging and auditing purposes must be specified before the design.

9.1.2 System approval

Criteria for the approval of new information systems, upgrading and new versions of current systems, must be stated and suitable tests of the systems must be conducted before approval.

9.2 System development

Security must be integrated into information systems used within FYEO to prevent losses, unauthorized modifications and data misuse in application systems.

9.2.1 Message verification

Message verification must be introduced to those applications where it is a security requirement to protect the integrity of the message contents.

9.2.2 Validation of output and input data

Output and input data must be validated to ensure that the processing of stored information is correct and in accordance with given assumptions. The validation process will detect if values are out-of-range, missing, incomplete or otherwise invalid.

Data should be validated at its source of creation to ensure all users of that data are provided with accurate data.

Systems should be designed to provide proof of integrity of important information and data records; electronic signatures should be used when integrity must be maintained.

9.3 Database and file security

Maintaining system integrity is the responsibility of the user or the development group to whom the application system or software belongs.

9.3.1 Protection of software data and source code

Data and software must be managed in a secure manner. Strict control and management must be practiced regarding the access to archives containing source code.

9.3.2 Development and maintenance

Application systems must be audited and properly tested before the system is changed. When modifying software packages, changes must be strictly managed. Purchase, usage and modifications of software must be managed and controlled for protection against any possible hidden channels and Trojan/Malware code.

Executable code may not be implemented on operational systems until successful testing and user acceptance is obtained.

10 Continuity management

There must be a managed proceeding regarding organization business to protect critical business proceeding from the effects of unpredictable, serious interrupts or catastrophes.

10.1 Contingency planning

Higher management has the responsibility to plan routines for continuing business in case of interruptions, and further to educate all employees in their roles in these plans and routines.

10.1.1 Continuity management process

A strategic plan based on suitable risk analysis must be developed to maintain the contingency of whole company business. Plans must be developed so that FYEO organization business can continue or be recovered within requisite time after an interrupt or failure in critical routines.

The consequences of disasters, security failures and loss of service should be analyzed and taken into consideration when creating a strategic contingency plan. The contingency plan must further be tested and updated on a regular basis.

Department managers are responsible for:

- Identifying critical business processes
- Assess the risks and their impact on the business
- Develop plans, emergency procedures and failback routines to be used in case of disastrous interruptions
- Decide what the conditions for activating the plans should be
- Test the plans and procedures

10.1.2 Testing and maintaining

A single framework regarding business contingency must be introduced to ensure that all plans are consistent and can be used for priority decisions regarding testing and maintenance.

11 Compliance

Information regarding internal systems or employees as well as customers must be protected according to current Swedish and Danish laws and regulations.

11.1 Legal requirements

It must be ensured that FYEO systems are in accordance with organization security policy and security standards and further, also in compliance with FYEO legal requirements.

Instruments of control must be introduced to protect data regarding individuals in accordance with relevant laws. Management must authorize all usage of information handling resources, and instruments of control must be used to prevent misuse of any kind regarding those resources.

Managers will ensure that all security procedures within their area of responsibility are carried out correctly.

11.1.1 Copyright

All business at FYEO must comply with copyright regulations, particularly when handling proprietary material and data of customers, suppliers and partners. Use of non-licensed software is not permitted and employees are not permitted to install or use personal software in any of FYEO's computers. Copying of software to CD-ROM, disk or USB for purpose other than backup is not permitted unless authorized by management.

Only material developed by FYEO or licensed or provided by the developer to FYEO may be used to avoid copyright infringements.

A register of company assets must be kept and updated on a regular basis.

11.1.2 Protection and privacy of personal data

Employees are not allowed to reveal personal information, like address or mobile number, to persons outside the FYEO organization without approval from the employee in question.

11.1.3 Protection and privacy of customer data

The Personal Data Act requires FYEO to obtain customers' approval and to inform them of how we are going to collect, process and share their personal data.

11.1.4 Reprimands

Reprimands will be placed on those disobeying current regulations, proceedings and routines within the company.

11.2 Adherence of security policy

Managers, within their own area of responsibility, must ensure that all routines regarding security are properly carried out and that all business areas are regularly audited to ensure the obedience of the security policy and security standards.

Information systems must be regularly audited regarding the obedience of standards for the introduction of security.

11.3 System audit

To ensure the compliance of FYEO systems and security policy, reviews of the information systems should be performed against the appropriate security policies.

Audit activities must be carefully planned and agreed to minimize the risk of disruptions to the business process of FYEO. This includes agreement with appropriate management of the audit requirements and scope. All audits must be documented thoroughly.

An annual system audit will be performed by a suitable outside organization to point out weaknesses and to continually develop and improve the overall security of FYEO.

11.3.1 Technical compliance

Information systems should be regularly checked for compliance with security implementation standards.