Sample Security Policy

Note: this sample policy is for informational use only. Before use, you should satisfy yourself that this policy is appropriate for your business and legal in your jurisdiction.

Table of Contents

Purpose

This document defines the complete security policy of Example Company Ltd ("ECL"). ECL takes the privacy of its employees and clients seriously, and in order to ensure that we are protecting our corporate and client data from physical and electronic security breaches this policy must be followed and will be enforced to the fullest extent.

Intent

The goal of this policy is to define the rules and procedures relating to security compliance.

The data covered by this policy includes, but is not limited to, all information found in e-mail, databases, applications and other media, including paper information, such as hard copies of electronic data, employee files, internal memos, and so on.

This document also covers the physical security of the building and its contents where relevant and reasonable.

Applicability

Audience

This policy applies to all employees, management, contractors, vendors, business partners and any other parties who have access to company data. This includes physical access to hard copy data and access to the premises where reasonable.

It is the responsibility of everyone who works at ECL to protect all data, whether it is electronic or otherwise. Even unintentional abuse of classified data will be considered a breach of contract and will be dealt with in accordance with the Company disciplinary procedures.

Notwithstanding the definitions below, data may be disclosed as follows:

- To those with a legal right to such data.
- To ECL's professional advisers who require such data to fulfil their obligations to ECL, and who have signed a Non Disclosure Agreement with ECL or who have a professional obligation to maintain confidentiality.
- Data regarding ECL's Security Policy may be disclosed to partners, clients, prospects and advisers provided that the recipient has signed a Non Disclosure Agreement with ECL.
- Client information may be disclosed to representatives of the client as required and as agreed by the client.

Equipment

This policy applies to all of ECL's production network, workstations and server equipment.

Confidentiality

All relevant parties are required to adhere to the Terms and Conditions as set out in this Policy document. It is likely that certain confidential data may be learned whilst executing normal duties. A Non Disclosure Agreement (NDA) must be completed by all relevant individuals/parties, and forms part of the Contract of Employment (employees) and the Contract of Services (contractors). All information and trade secrets must be:

1. Kept secure at all times
2. Used in accordance with the Company Security Policy document
3. Not divulged or communicated to unauthorized individuals/parties

The contractual clauses covering these restrictions persist after the contract has terminated.

Responsibilities

All employees are responsible for adhering to the Company security policy and reporting any activities that do not comply with this policy, including unauthorised physical access to the Company premises. Any observed or suspected weaknesses in security are to be reported by email to security@example.com.

Managers are responsible for ensuring:

- that their direct reports understand the scope and implications of this policy
- the compliance with the company security policies of information processing and procedures within their area of responsibility
- the security procedures applicable to their area of responsibility are reviewed at least annually

The definitive version of this Company security policy is held on the Company Intranet.

Security measures

The following methodologies are used by ECL in order to protect all data:

Employees

Every employee's Contract of Employment includes confidentiality clauses that survive the termination of the contract.

Physical Security

1. Access to premises is overseen by means of CCTV cameras operated by the company.
2. A security alarm is fitted.
3. A building access control system is in place with keyless entry for authorised personnel.
4. The building access control system maintains a record of who enters the building together with the time and date of entry.
5. The production network switches, server and routers are all kept in locked rooms.
6. All employees' access rights to the premises etc are terminated immediately upon leaving employment of the Company.
7. All paper documents, are to be placed in steel filing cabinets and kept locked when not in use by the relevant authorised personnel.
8. Filing cabinet keys are to be removed at the end of the working period and retained by appointed staff.
9. The dedicated server room is to be kept locked when unattended.

Electronic Security

Authentication

Access to Confidential Information requires authentication credentials (username/password unless otherwise noted).

Command line access to computer systems, including client systems but excluding staff personal workstations, requires Two Factor Authentication.

Two Factor Authentication

Two factor authentication requires possession of a physical device (a 'token') and knowledge of an individual passphrase.

Physical tokens must have both user and administrative level functions, and both must be protected by a passphrase. Access to add, remove or change data on the token must be restricted to an administrative level. Physical tokens must not be shared among users but are issued by the Company for individual use only.

Administrative passphrases are known by System Security Administrators only and must be treated by them as Confidential. User passphrases must be user-selected and known only to the assigned user. User passphrases for tokens used by System Security Administrators must be distinct from any administrative passphrase. The physical token must not function without presentation of the user or administrative passphrase. Loss or compromise of a

physical token must be reported promptly to the Information Security Manager.

Physical tokens must not permit any person to access the secret material stored on them; a "write-once read-never" approach must be taken.

Password and Pass Phrase Policy

All user accounts must be password or pass phrase protected. Passwords and pass phrases must be either a) a minimum of 8 characters and include at least four of the following; or b) a minimum of 15 characters and include at least three of the following:

- upper case characters
- lower case characters
- numeric characters
- punctuation characters
- non-alphanumeric, non-punctuation characters (eg, "%", "@" or "*")

Passwords must not be written down. They may be retained electronically provided that they are encrypted to at least 256-bit key Advanced Encryption Standard (“256-bit AES”) and are protected by a password or passphrase that meets the above requirements.

Individual passwords and passphrases must not be divulged.

Username Policy

Usernames for ECL systems must uniquely identify an individual.

Workstation Security

- All employee workstations must have an automatic session lock which activates after 5 minutes or less of inactivity.
- Users are responsible for safeguarding their passwords for the system.
- Access to the Internet via the Company's computer system is provided for the purposes of the User's employment or engagement by the Company. Use of the Internet for any other purpose is therefore strictly prohibited with the exception of reasonable use in accordance with this Policy outside User's working hours.
- Appropriate licences must be held for all software loaded on the Company's equipment. The Company strictly forbids Users from using any illegal copies of software.
- Confidential or highly sensitive messages must not be sent by email unless encryption is used.

- Workstation users are required to conform with the Acceptable Use Policy contained within the Employee Handbook.

Network and Server Security

- Connections to company servers may only be via encrypted protocols (ssh, IMAP with TLS, HTTPS, etc). SSL/TLS certificates used to secure publicly-accessible services provided by ECL must be Public Key Certificates (not self-signed certificates).
- All server passwords are kept in the appropriate Company Password Database, and are encrypted to AES256 standards. Only personnel who have a need to use those passwords are to have access to the Password Database.
- No equipment is to be connected to the Company Network unless necessary to access Company resources. In particular, this means that visitors are not to connect any equipment to the Company Network.
- A "guest" network may be provided and this may be used by visitors at the discretion of the Information Security Manger. Any guest network must be firewalled from accessing the Company Network. In the case of a Wireless Network, a time limited "Guest Voucher" is required and only the minimum appropriate time is to be authorised by any employee.
- All electronic equipment that is not already installed or part of the existing office equipment is subject to an investigation (reasons why it is required and what it actually is and does) by the Company Information Security Manager or other designated staff.
- Access to all Company computer servers/routers/network switches/hubs and cabling is restricted to qualified and authorized personnel only.
- All ECL servers are to be backed up in full every night to two independent backup servers, located in geographically disperse data centres managed by different companies.
- All servers are to run an appropriate system logging utility; unexpected log entries are to be examined and appropriate action taken. Logs must only be accessible to system administrators.
- All servers are to run a Network Time Protocol client to keep the system clock in time.

All servers are monitored to ensure (amongst other things) that:

- all relevant security updates are installed in a timely fashion
- system backups are up to date and complete
- system performance is adequate for the role
- security certificates have at least 10 days' validity

- the system clock is within 0.5 seconds of an Internet reference time source

Server Upgrades and Replacements

Following an operating system upgrade or server replacement, the following shall be carried out:

- server monitoring to be reviewed for appropriateness and completeness
- server monitoring to be checked for indications of any problems or potential problems
- the Information Security Manager must ensure that all applications have been tested prior to (re-)acceptance of the server into production use

Malware

Incoming email is scanned for viruses, and any found are removed.

Linux servers and Linux workstations are not expected to routinely run antivirus software.

Internal Applications

ECL makes use of internal applications, some authored entirely in-house and some which are Open Source applications, possibly with in-house modifications. The following applies to all applications written or modified by the Company.

- All source code is to be stored in the Company source code repository.
- Write access to the Company source code repository is by Two Factor Authentication, outlined above.
- Changes to applications are to be reviewed and authorised by a System Security Administrator uninvolved in the code changes.
- Change Requests are to be recorded and managed using an appropriate tracking or ticketing system.

Configuration Management Server

All internal production servers are managed using ECL's Configuration Management Server.

Handling of configuration files managed by the Configuration Management Server is to follow the requirements above for "Internal Applications"; in addition, the following points apply to Configuration Management Server changes that implement significant functionality to a server or servers. Such changes are to be developed in a separate source code control testing branch. The changes are to be tested as follows:

- The changes are implemented on an internal test environment or, with the client's consent, on their test environment.
- User Acceptance Testing (UAT) is undertaken by relevant personnel.
- Any faults or issues are referred back to the change author for rectification.
- Once testing is complete, changes are to be reviewed and authorised by a System Security Administrator; where possible, the System Security Administrator should have been uninvolved in the changes.
- A roll-out schedule is agreed with the department manager.

To maintain an effective audit trail, the following is implemented:

- Changes to the configuration management application itself, including files that are distributed to managed servers, are to be submitted via the established source code repository.
- root logins to the configuration management server are restricted to Security Administrators and Directors of the company.

Physical waste

- All paper waste containing sensitive data is shredded in a cross-cut shredder.
- Hardware components that may contain sensitive data (typically disks) are dealt with as follows:
  - If the component is serviceable, the data is securely erased.
  - If the component is not serviceable, it is physically destroyed.

Staff

Induction And Training

Upon commencement of employment, induction training is provided to the new member of staff before they commence their actual duties. This induction covers the following:

1. Security, both physical and electronic
2. Internal and external applications
3. Policies and Procedures
4. Employment terms and conditions
5. General issues covering legal requirements

Staff training is reviewed quarterly at the monthly management meeting, and additional training is given as required.

Granting Of Access

Staff will be granted access to data only as required to fulfil their obligations. Requests to grant access are handled as follows:

- If the initial request is raised by someone other than the employee's manager, it should first be made by email to the employee's manager
- The manager should ascertain that the employee does need such access and, if satisfied, forward the request to the Information Security Manager
- If satisfied that the request is appropriate, the Information Security Manager will arrange for the access to be granted.

Termination

When staff leave, or when an agreement with an external contractor is terminated, the Information Security Manager is responsible for ensuring that the leavers checklist procedure is followed.