

INFORMATION

SECURITY

POLICY

**Information Security Policy**

1. **Purpose**

The Information Security Policy is intended to guide employees and sub contractors in determining what information can be disclosed outside of [INSERT BUSINESS NAME] without proper authorisation.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees and sub contractors should familiarise themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasise common sense steps that you can take to protect XXX Confidential information (e.g., XXX Confidential information should not be left unattended in conference rooms).

1. **Scope**

All XXX information is categorized into two main classifications:

* XXX Public
* XXX Confidential including DBS Documentation

XXX Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to [INSERT BUSINESS NAME].

XXX Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as investigation files and client information. Also included in XXX Confidential is information that is less critical, such as internal telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of XXX Confidential information is "XXX Third Party Confidential" information. This is confidential information belonging or pertaining to another client or corporation which has been entrusted to XXX by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development projects to case investigation files, personal information, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into [INSERT BUSINESS NAME]'s network to support our operations.

In the case of “XXX Third Party Confidential” information, the measures to be adopted in protecting this information should be those contained within this XXX policy or those imposed by the third party within its own organisation, whichever are the most stringent.

XXX personnel are encouraged to use common sense judgment in securing XXX Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact the Business Principal.

1. **Policy**

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as XXX Confidential information in each category may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the XXX Confidential information in question.

* 1. **RESTRICTED:** General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words **"XXX RESTRICTED"** should be written or designated in a conspicuous place on or in the information in question.

**Access:** XXX employees, contractors, people with a business need to know.

**Distribution within XXX:** Standard interoffice mail, approved electronic mail and electronic file transmission methods.

**Distribution outside of XXX internal mail**: Royal Mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

**Electronic distribution:** No restrictions except that it be sent to only approved recipients.

**Storage:** Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

**Disposal/Destruction:** Deposit outdated paper information in specially marked disposal bins on XXX premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

* 1. **CONFIDENTIAL:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words **"XXX CONFIDENTIAL"** should be written or designated in a conspicuous place on or in the information in question

**Access**: XXX employees and non-employees with signed non-disclosure agreements who have a business need to know.

**Distribution within XXX:** Standard interoffice mail, approved electronic mail and electronic file transmission methods.

**Distribution outside of XXX internal mail**: Sent via Royal Mail or approved private carriers.

**Electronic distribution:** No restrictions to approved recipients within [INSERT BUSINESS NAME], but should be encrypted or sent via a private link to approved recipients outside of XXX premises.

**Storage:** Individual access controls are highly recommended for electronic information.

**Disposal/Destruction:** In specially marked disposal bins on XXX premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

* 1. **SECRET:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words **"XXX SECRET"** should be written or designated in a conspicuous place on or in the information in question

**Access:** Only those individuals (XXX employees and non-employees) designated with approved access and signed non-disclosure agreements.

**Distribution within XXX:** Delivered direct - signature required, envelopes stamped Secret, or approved electronic file transmission methods.

**Distribution outside of XXX internal mail:** Delivered direct; signature required; approved private carriers.

**Electronic distribution:** No restrictions to approved recipients within MIL, but it is highly recommended that all information be strongly encrypted.

**Storage:** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

**Disposal/Destruction:** Strongly Encouraged: In specially marked disposal bins on XXX premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

1. **Enforcement**

Any employee or sub contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1. **Definitions**

**Terms and Definitions**

**Appropriate measures**

To minimise risk to XXX from an outside business connection. XXX computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access XXX corporate information, the amount of information at risk is minimized.

**Configuration of XXX-to-other business connections**

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

**Delivered Direct; Signature Required**

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

**Approved Electronic File Transmission Methods**

Includes supported FTP clients and Web browsers.

**Envelopes Stamped Secret or Confidential**

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it as appropriate.

**Approved Electronic Mail**

Includes all mail systems with which XXX has e-mail access.

**Approved Encrypted email and files**

XXX uses HUSHMAIL.

**Company Information System Resources**

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

**Expunge**

To reliably erase or expunge data on a PC XXX Uses INVISIBLE SECRETS software.

**Insecure Internet Links**

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of [INSERT BUSINESS NAME]. If necessary to cloak an IP Address, XXX uses HMA software.

**Encryption**

Secure XXX Sensitive information by using Truecrypt or Bestcrypt software and encrypted removable hard drives.

**Physical Security**

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.