POLICY J

DATA SECURITY POLICY

Objectives

The objectives of this policy are to:

- Ensure that IT facilities are adequately protected against loss, misuse or abuse.
- Raise awareness of IT security issues throughout the Company and to ensure that they are considered at every stage of an IT system life cycle.
- Ensure that users understand their responsibilities for protecting the data they handle.

Compliance with Legislation

The Company has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures and standards satisfy the requirement under the Data Protection Act 1998 and The General Data Protection Regulation (GDPR) 2018.

Equipment and Software used by Individuals and Workgroups

The following policies apply to equipment and software which is used by an individual or shared by a group of users. Examples of equipment to which this policy applies are telephone handsets, AV equipment, desktop and laptop computers, individual and shared printers, photocopiers.

Specification and selection of IT equipment must be done by or in consultation with the IT Department.

The IT Department will maintain a record of all software licences it purchases.

Installation and upgrading of individual and workgroup equipment and software will normally be undertaken by the IT Department or its approved contractor.

No user may install additional hardware, software or alter the configuration of any IT equipment except:

- IT Department staff and other authorised personnel may install hardware, software or alter equipment configuration for testing and evaluation.
- Where hardware or software has been procured via the IT Department and is accompanied by adequate instructions for installation, the hardware or software may, by mutual agreement, be given to the user for them to install. This shall be deemed as authorisation to install only this item.
- Auto-updating software (e.g. virus signature files) originally installed and configured by the IT Department may continue to install updates under the authority of the IT Department.

If hardware or software, other than updates to existing software, is acquired by a member of staff other than via the IT Department (e.g. by personal purchase or download from the Internet), that member of staff may only install it after consulting the IT Department for known issues concerning that hardware or software.

Portable computers belonging to users or their employers may be connected to the Company network provided that the software is adequately patched and it is protected from infection by malicious software and from transmitting malicious software to other systems.

The installer must ensure that data is backed up before installing additional hardware or software.

No licence agreement may be entered into if the consequences or potential consequences will adversely affect performance or incur direct or indirect costs for the Company unless authorised by the IT Department.

All installations and upgrades must be within the terms of the licence agreement and must be deleted in accordance with the licence.

Every user must ensure the correct use and adequate safeguarding of data for which they are responsible. This includes suitable backups of the data.

All portable equipment and software shall have a designated user. The designated user is the person with whom the equipment is normally lodged and this person is responsible for the security of the equipment and software. The designated user, the designated user's line manager, and the IT Department have the ability to authorise the use of that portable equipment and software outside of Company premises.

Equipment on temporary loan to a named individual will make that individual responsible for the security, correct operation and condition of the equipment, and for its return in good condition within the agree period of the loan. Failure to return the equipment by the end of the loan period will be considered as theft.

No equipment may be taken off Company premises without the consent of the CTO or his designated deputy.

All redundant equipment and software must be passed to the IT Department for redeployment or for disposal.

Accounts on the network

Resources for the maintenance and support of IT equipment and software will be managed based on the needs of the Company as a whole. Priority will be given to maintenance and support of equipment and software that is widespread or critical in nature. Lower priority will be given where equipment or software is older, less widespread or non-critical to the Company.

Health and safety

All equipment connected to the Company's network must conform to the Company's Health and Safety Policy.

Connection to Cognisco's network

Only approved equipment may be connected to or used to access the Company's network. *In particular, no wireless access points may be connected to the network without approval.*

Operating procedures and conditions for all connected equipment must be approved by the Chief Technology Officer.

Connection of equipment to the Company's network shall only be performed by staff from the IT Department or approved contractors.

Remote access to Cognisco's network

Remote access for users to the Company's network will normally be via the Internet and is only permitted for the retrieval of e-mail and information from designated servers.
No user may set up or maintain a private dial-up connection into the Company's IT resources.

Use of e-mail

E-mail systems are provided for the conduct of Company related business. Incidental and personal use of e-mail is permitted so long as such use does not disrupt or distract the individual from Company business (due to volume, frequency or time expended), does not incur unreasonable cost to the Company, and/or does not restrict the use of those systems to other legitimate users. Users are reminded that the IT Department can access their e-mail messages for operational and security purpose.

Anonymous accounts will not be allowed on Company systems. Anonymous accounts do not allow proper management, accountability or traceability and would inherently contravene IT Policies.

The Company network and e-mail systems may not be used to transmit:

- Material unrelated to Company business including bulk e-mail transmissions (SPAM).
- Messages requesting the recipient to continue forwarding the message to others, where the message has no relevant value.
- Messages with forged addresses (spoofing) or otherwise purporting to come from a source other than the true sender.
- All messages distributed via the Company's email system, even personal e-mails, are the Company's property.

Use of the Worldwide Web

Access to the Worldwide Web (Web) is provided for research, teaching, learning and other legitimate Company related business. Incidental and personal use of the Web is permitted so long as such use does not disrupt or distract the individual from Company business (due to volume, frequency or time expended), does not incur unreasonable cost to the Company, and/or does not restrict the use of those systems to other legitimate users.

The Company will provide a default home page for all browsers on its owned or leased equipment. Users must not alter this home page without legitimate reason.

It is the responsibility of the member of staff authoring the pages to comply with Company policies regarding content, presentation, accessibility, data protection and security.

Pages containing dynamic content must have the involvement of the IT Department in their development and approval for their compliance with policies. "Dynamic content" means that the page's content may change either by user interaction or by changes in the source data used in the page.

Examples of dynamic pages are: pages that rely on an element of programming for their content; pages that accept input from users; pages that use a database as their source of information.

Use of telephones

The Company's telephone systems are provided for Company related business. Incidental and personal use of the telephones is permitted so long as such use does not disrupt or distract the individual from Company business (due to volume, frequency or time expended), does not incur unreasonable cost to the Company, and/or does not restrict the use of those systems to other legitimate users.

Where exceptional personal circumstances may lead to infringement of this policy, users should agree with their line manager the acceptability of their telephone usage.

Each mobile phone shall have a registered user and that user will be responsible for the use and security of the phone. The registered user must report the loss of or any damage to their phone to the IT Department.

Use of facsimile machines

The Company provides facsimile machines for Company related business. Incidental and personal use of fax is permitted so long as such use does not disrupt or distract the individual from Company business (due to volume, frequency or time expended), does not incur unreasonable cost to the Company, and/or does not restrict the use of those systems to other legitimate users.

Use of photocopying and printing equipment

The Company provides photocopiers and printers for Company related business. Incidental and personal use of photocopiers and printers is permitted so long as such use does not disrupt or distract the individual from Company business (due to volume, frequency or time expended), does not incur unreasonable cost to the Company, and/or does not restrict the use of those systems to other legitimate users.

IT purchasing policy

All procurement of IT equipment, software and services for the Company must be made either through the IT Department or in full consultation with the relevant personnel in the IT Department. The IT Department may veto a purchase or lease if it believes that IT policies have been breached.

For standard equipment, software and services, purchases will be through the appropriate process of obtaining three quotes. IT equipment, software and services for the Company will be purchased on the basis of best value for money over the complete life cycle of the goods. Initial cost is not the only criterion to be considered: support requirements, warranties, reliability of goods as well as suppliers, longevity, and disposal costs must also be considered.

Where a non-IT Department budget is being used to fund a purchase or lease, it is the budget-holder's responsibility to ensure that sufficient funds are available for the purchase and that all relevant information is supplied to the IT Department to facilitate the purchase/lease.

Disposal of IT equipment

All equipment will be disposed of in compliance with current legislation and with due regard for social and environmental considerations.

Disposal shall not expose the Company to continuing commitment to support or maintain any systems.

Disposal of equipment shall constitute best value to the Company.

Where equipment has no residual value, recycling of materials or components shall be done in as economical a way as possible.

Non-compliance with these policies

Illegal activities

Infringements of the relevant legislation will result in legal and/or disciplinary action. All such infringements must be reported to the CTO or the CEO. The Company maintains a Whistle-blowing policy. Please see policy N.

Breaches of Company policies

Correcting problems caused by a breach of IT policies will be done at minimum effort and cost to the Company. The Company reserves the right to pass on some or all of the cost involved to those causing the breach.

Consequences of violations of the IT Policy will depend on the intent, the seriousness of the offence and the damage caused. All such violations must be reported to the Chief Technology Officer or the CEO. The Chief Technology Officer will follow disciplinary procedures for more serious offences.

IT Department staff may disconnect equipment without notice if it is believed that IT Policies are breached while an appropriate investigation is carried out.

Breach of Policies by employees may result in suspension of access to IT equipment and services for minor breaches, or formal disciplinary action, which may result in dismissal, for more serious offences.