Information and Communication Technology Use and Information Security Policy/Data Protection

A. Information and Communication Technology Use

All information and communications technology users, irrespective of their employment status, are required to adhere strictly to this policy.

1 Any and all data created, altered or received on any piece of Company equipment is the property of the Company and may be monitored, read, stored, manipulated or used as the Company sees fit. This includes any and all emails sent and received and any other internet use.

2 With the following exception, the Company's computer equipment must not be used for any purpose other than Company business without the consent of the Systems Manager.

Exception to Rule 2: personal use of email and the internet is allowed provided that such use is kept to a minimum and that only a reasonable amount of the Company's time and resources are used. In particular:

- no references may be made to the Company, and no implication may be made that you are expressing the Company's views
- no bulk mailings may be sent
- no content which might infringe any part of this or any other company policy may be created, viewed or sent (including forwarding).

3 No user should use Company systems to create, view or send (including forwarding) any material that is or might be construed to be abusive, sexist, racist, defamatory, harassing or otherwise offensive. Such action could have legal consequences for the user and the Company.

4 The data that the Company holds on living people is subject to the Data Protection Act. This requires all computer users to keep such data safe and not disclose it to any unauthorised persons, either in person, in writing, by telephone or any other means. No data should be revealed to any party outside of the terms of the Data Protection registration held by the Company. If in doubt, seek clarification from the Systems Manager. Even if revealing such information would not breach the Data Protection Act, the Company's staff members have a duty not to reveal or disclose any data or information that may cause damage, loss or embarrassment to any party, e.g. to the Company or its customers, suppliers or other contacts.

5 No user should knowingly break any law, or attempt to do so, using any piece of Company equipment.

6 No system settings should be altered on any system without the permission of the Systems Manager. This includes items such as communication settings, file locations, default printer drivers, etc. Users must remember that the systems are complex and interdependent, and altering any setting can have unforeseen consequences.

7 All users must be aware that certain types of computer file, such as executable files and many types of document file (including Word documents), can contain viruses which can cause severe damage. Such files may be recognised by unusual file extensions. The Company's systems have up to date anti-virus software which gives some protection. However, a new virus can travel extremely quickly and can infect computer systems before the anti-virus software has been updated to deal with it, so vigilance is always necessary. Note that some viruses have come to light in email attachments named, for example, attach.txt.exe, which some persons have opened in error believing that it was a text file.

8 Unless covered by the exceptions below, no user should use or attempt to use any unauthorised disks, USBs or other computerised material, or install or attempt to install any software from any source, on any Company computer system without the permission of the Systems Manager. This includes newly purchased software, downloading of software or data of any description from the internet or other services, or opening any attachment received in an email. Should you suspect that this has taken place either by another user or (perhaps inadvertently) by yourself, you must inform the Systems Manager immediately and must not use the suspect system until given permission to do so.

Exceptions: It is acceptable to proceed with downloads of known system updates, e.g., updates to software that is known to be installed. Otherwise, it is acceptable to use disks and other removable media, open email attachments or download items provided that they conform to ***all*** of the following requirements:

Disks and other removable media
- a the disk/media must be from a known and trusted source
- b the complete contents of the disk/media must be fully virus checked by *trained* Company staff, on the Company systems, whilst on the Company premises
- c no executable files (e.g., with extensions of .exe, .com or .zip) are to be opened without the permission of the Systems Manager
- d no files which are suspected to be anything other than document files are to be opened without the permission of the Systems Manager

Email Attachments:
- a the email must be from a known and trusted source
- b attachments with unusual extensions such as .cvf should not be opened without the permission of the Systems Manager
- c no attachments which are suspected to be anything other than document files are to be opened without the permission of the Systems Manager. If in doubt, do not open – check with the Systems Manager

Downloads:
- a the download must be from a known and trusted web site or other location
- b the download must be initiated by the user – downloads suggested by the system must be refused or referred to the Systems Manager
- c the user must be fully confident that the download is a document, not an executable file

9 Passwords must not be revealed to any unauthorised person. Personal passwords, i.e., those which are personal to you and are not used by others, must not be disclosed to ***any*** person other than the Systems Manager. If you suspect that a password has become known to another person, you must inform the Systems Manager immediately.

10 Users must log off before leaving a personal password protected system unattended. When requiring access to a personal password protected system which is already running under another person's logon, the system must be logged off and the user must log on with their own password.

11 It is acceptable to leave a common password protected system (where all users use the same password) unattended, provided that another user who could access it with the same password is present. Should no other such user be present, the system must be logged off.

11 No person should attempt to use a password belonging to another person or otherwise attempt to gain unauthorised access to any computer data without permission from the Systems Manager. Such action may be an offence under the Computer Misuse Act 1990.

12 No person should attempt to gain unauthorised access to any part of any system which they would not normally be expected to use, or to attempt to circumvent any security feature in any system.

13 All users should be aware that backups of Company computer data are made daily. As the deletion of computer data by individual users does not necessarily remove the data from all locations, all computer users should be aware that this material may be held on computer systems and/or included in any archives which could be reconstructed later should the need or obligation arise.

14 Email, whilst being a less formal method of communication then by letter, is an official communication from the Company and can be produced as evidence in a court of law. The content of emails should be composed with the same care as would be given to a letter on company notepaper.

15 Any and all system errors should be reported to the Systems Manager with as complete as is possible an account of the circumstances of the error, including the exact text of any error messages given by the system.

16 Any accidents causing, or suspected to cause, any damage to either the hardware, software or configuration of any system should be reported to the Systems Manager with as complete as is possible an account of the circumstances of the incident.

17 No Company computer equipment should be removed from the premises without the permission of the Systems Manager, or Quality Manager.

18 Any breach of any part of this policy may lead to disciplinary action, and possibly termination of employment.

If in doubt contact Integer's System Manager, Jake Thompson, at jakethompson@integer.co.uk or call 07368 668684

B. Information Security/Data Protection

1. Scope: This policy covers all electronic information storage and processing carried out by the Company.

2. Legal and regulatory obligations: the Company complies with the requirements of the Data Protection Act, GDPR and the Privacy and Electronic Communications Regulations.

3. Roles and responsibilities: All staff members are responsible for information security.

4. Strategic approach and principles: Data is held in commercial cloud services. Staff members are given access to this data at a number of levels of permission, giving them access to information that is required and relevant for their job role. We may also hold some data in shared cloud services, for example Dropbox and OneDrive, for the purpose of sharing with other parties. Where the share is initiated by Integer, access to these shared resources is restricted to certain known parties by the member of Integer staff responsible for the share.

5. Action in the event of a policy breach: Policy breaches are taken seriously by the Company. The typical responses would be:
    - Loss (deletion) of data would be rectified with use of data backups.
    - Leakage of data (to unauthorised parties) would prompt a range of responses, including investigation to discover the extent of the leak and contacting affected individuals to inform them of the leak.

6. Access control: All access to data is controlled through use of user accounts and passwords on the network. Different users have different access rights. All staff members are instructed to lock their workstations when leaving them unattended, and all workstations automatically lapse into password protected sleep after a set period of inactivity as an extra security measure. Computer access and user activity logs are kept.

7. Operations: Staff login to their workstations on arrival, lock their workstations when leaving them temporarily unattended and log off when leaving. Staff members do not share passwords or logged-in systems. Password changes are enforced annually, and a security policy requires strong passwords. Staff members are instructed not to write passwords down. Individual data systems which are accessible through workstations are individually password protected.

   All staff members are aware that the sharing of personal information is regulated by legislation and that where there is any doubt they should seek guidance from the Systems Manager.

   Where the Company website invites persons to submit personal details through a web form, this will take place using an SSL certificate over a secure, https: connection.

Staff members are instructed that, even if the Company email system is not functioning, they must never use their own personal email accounts to transmit or receive personal information related to the company or its work.

Individuals have certain rights to have access to personal data that we hold on them. Should such a request be received (a “data access request”), it should be referred to the Systems Manager.

8. Physical security: Computers are located in offices which are locked in an intruder alarm protected building when unattended.

9. Business continuity management: We have a robust data backup regime which could reinstate our systems quickly in the event of a major disaster.

The Data Protection Act 2018 covers any information that relates to living individuals which is held on computer. For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified.

Integer is committed to ensuring that the use of personal data is fully compliant with the law and best practice. We therefore comply with the Data Protection principles that state that personal information is:

- fairly and lawfully processed
- processed for specified purposes
- adequate, relevant and not excessive
- accurate and, where necessary, kept up to date
- not kept for longer than is necessary
- processed in line with the rights of the individual
- kept secure
- not transferred to countries outside the European Economic Area unless the information is adequately protected

Responding to requests for personal information: Where a request to disclose personal information is received, the following checks must be made before providing the information:

- ensure that the person making the request is entitled to receive the information requested
- establish the identity of the person making the request

Disposing of printouts etc. containing personal data: Such items must be securely disposed of, e.g., by confidential data disposal company.

Sending personal data by email: Where it is necessary to send personal data by email, the data must be in an encrypted attachment, not in the body of the email itself. To encrypt Word or Excel documents, simply apply a password to open the file. The password must be supplied to the recipient of the email, although it must not be sent in the email itself.

1. Ensure that files are encrypted to AES 256 bit encryption standards using WinZip version12 or higher.
2. Create and use a passphrase with a minimum of 15 alpha-numerical characters including symbols, for example: He0H0wAr3yT0d?
3. After emailing your encrypted files, you must communicate the password via a further email or by telephone.

If in doubt contact Integer’s System Manager, Jake Thompson, at jakethompson@integer.co.uk or call 07368 668684

C. Social Media

This provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

The following principles apply to professional use of social media on behalf of Integer as well as personal use of social media when referencing Integer.

- Employees need to know and adhere to Integer's Code of Conduct and other company policies when using social media in reference to Integer.
- Employees should be aware of the effect their actions may have on their images, as well Integer's image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that Integer may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Integer, its employees, or customers.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.
- Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with Human Resources and/or their manager.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorised Integer spokespersons.
- If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at Integer. Integer's computer systems are to be used for business purposes only. When using Integer's computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Integer's blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Subject to applicable law, after-hours online activity that violates Integer's Code of Conduct or any other company policy may subject an employee to disciplinary action or termination.
- If employees publish content after-hours that involves work or subjects associated with Integer, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent Integer's positions, strategies or opinions."
- It is highly recommended that employees keep Integer related social media accounts separate from personal accounts, if practical.

If in doubt contact Integer's System Manager, Jake Thompson, at jakethompson@integer.co.uk or call 07368 668684

DECLARATION

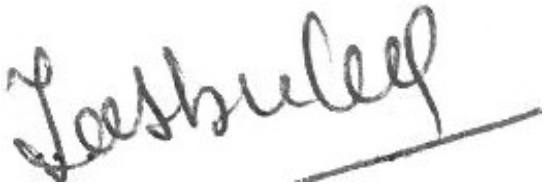
I confirm that I have read this policy and agree

Name of employee: …….

Signature: ……

Date: ……..

Declaration: I will review and revise this policy as necessary and at regular intervals:



Signature of Jasbir Behal, Managing Director, Integer Training Ltd

Date: 8 January 2025

Version No: ICT22011401

Review Date: 08/01/2026