Information Security Policy

Date issued: July 2024
Version: 14
Owner: Head of IT

Why do we need this policy?

Information, and the information technology (IT) and communications facilities that support it, are critically important business assets. Their availability, integrity and confidentiality are vital to Business Stream's effective operation.

Business Stream is committed to using and maintaining good information security practices by:

- Making sure we comply with all IT and security-related laws.
- Ensuring our IT assets, such as hardware, software, infrastructure and data, are protected against security threats.
- Creating and maintaining awareness of the need to secure these assets as part of our everyday work.
- Establishing an effective Business Stream Information Security Policy.

All authorised personnel, including employees, contractors, secondees, consultants, and agency staff, are granted access to the necessary IT and communication facilities for effective job performance. Third-party service providers are granted access to fulfil contractual obligations. Users directly impact the availability, integrity, and confidentiality of Business Stream's information and systems, and are accountable for actions logged under their username.

Using IT improperly could have adverse consequences for Business Stream, third party service providers and the individuals who use these systems. Information security is everyone's responsibility. As a responsible organisation, Business Stream regularly monitors the use of the information technology and communications facilities to ensure that the Information Security Policy is being adhered to.

What this policy covers

The use of Business Stream's information technology and communication facilities.

1. Important information

Everyone who uses Business Stream information technology and communications facilities must ensure that they understand the Information Security Policy and Practices, and any other associated guidelines, and fully comply with them.

Any instances of suspected or actual misuse of IT, whether intentional or not, which may compromise this policy must be reported to the Business Stream's IT Helpdesk immediately. Outsourced service providers should formally notify such instances to Business Stream's IT Helpdesk.

Failure to comply with this policy may lead to disciplinary action.

Consultants, contractors or outsourced service providers who fail to comply with this policy risk having their contract with Business Stream terminated.

2. Information technology and communications facilities

Business Stream provides information technology and communications facilities to fulfil its business needs. This includes mobile devices (laptops, tablets, mobile phones), desktop computers, phone systems, Internet / Intranet access, corporate email, business applications and the security infrastructure (networks, servers) to support these services.

The use of these systems must be professional, lawful and ethical, and must not disrupt the operation of the system for others, nor compromise this policy.

The storage of Business Stream information assets is strictly limited to Business Stream company computing equipment and approved information storage services. The storage of Business Stream company information on personal computing devices is strictly prohibited.

A certain amount of limited and responsible personal use is permitted subject to the control of your line manager and only during break times. However, the systems must not be used for political or your own commercial business purposes.

- Non-business-related multimedia data such as personal photos, videos and music must not be stored or transmitted using Business Stream's information technology and communications facilities.
- Any personal files (CVs, expenses, letters etc.) must be kept to a minimum and clearly labelled as personal.
- Business Stream's computers have a standard configuration. Changes to this configuration may only be made by Business Stream IT or by its IT service provider.
- All computer hardware and software must be acquired, installed and disposed of by Business Stream IT or by its IT service provider and its authorised partners.

Business Stream IT maintain an inventory of all information technology assets. Business Stream's IT Helpdesk should be informed if equipment has to be moved or if new software needs to be in installed. This includes any software available free or chargeable from the Internet.

All data received from out with Business Stream will be scanned for viruses before being stored on Business Stream systems. Normally this will be done automatically. Any user with concerns about this process or anyone who identifies a virus must contact Business Stream's IT Helpdesk immediately for advice.

Where line management has agreed that you can use IT equipment or data off-site for business-related activities, you must ensure that it is adequately secured in accordance with the Mobile Computing Policy.

2.1. Examples of forbidden activities

This list is not exhaustive but includes:

- deliberate unauthorised entry to systems (e.g. hacking)
- sharing of usernames, passwords and login details
- use of, or installation of unauthorised software
- use of systems for harassment of others
- unauthorised change of systems, software and data
- accessing, copying or distribution of sexual, pornographic, offensive or illegal material
- using any images, texts or materials which are copyright-protected, other than in accordance with the terms of the licence under which you were permitted to download them
- seeking to gain access to restricted areas of Business Stream's network
- the copying or removal of company information onto personal storage devices or services

The Business Stream IT Helpdesk should be consulted if there is any doubt on whether a specific activity is permitted or not.

3. Messaging and Calendar Scheduling

Email, messaging, collaboration and calendar scheduling services are provided to facilitate business activities. Careful consideration should be given to the type of information shared, the security of the information shared and the intended audience of the information shared.

3.1. Email and Messaging

All email and instant messages, sent or received, internally or externally, are the property of Business Stream.

Business Stream messages may only be stored using company owned IT equipment. The storage of Business Stream messages on personal computing devices is strictly prohibited. Any exceptions to this must be approved in writing by the Head of IT.

Business Stream reserves the right to access and disclose as it deems necessary, all messages sent or received via the company email and/or messaging systems.

You must make sure that the messages you send are not defamatory, offensive or discriminatory. Do not send anything in a message that would not be considered suitable in a memo or letter.

Email messages may have to be disclosed in litigation and may be read out in court. Except where there is a statutory exemption, any information held by Business Stream may be required for disclosure in response to a Freedom of Information request. This includes email and instant messages.

Consideration should be given to determine if email is the most appropriate form of communication for a message. Internal Communications should be consulted for advice on communication or if a communication needs to be sent to 'All users'.

A certain amount of limited and responsible personal use of the email system is permitted subject to line manager approval. Any personal use of Business Stream's email system:

- must not interfere with the performance of work duties
- must not take priority over work responsibilities

- must not cause unwarranted expense or liability to be incurred by Business Stream
- must not have a negative impact on Business Stream in any way
- must be lawful and comply with this policy.

Use of Business Stream's email or messaging systems for personal use does not imply any expectation of privacy as Business Stream needs to monitor all communications. To help identify personal emails as private they must be marked PERSONAL in the subject heading, and all personal emails sent or received must be filed in a folder marked "Personal" in your mailbox.

3.2. Calendar & Scheduling

Careful consideration should be given when sharing access to calendars and sharing information via calendar appointment invitations. Confidential or restricted information must not be included as part of a calendar appointment. Particularly sensitive information should be secured in a common shared area or issued directly to the intended recipient.

4. Internet

Access to Internet services is provided for the primary purpose of supporting business activities.

Non-work-related programs, files or streaming media must not be downloaded from the Internet without the permission of Business Stream's IT Helpdesk.

Material containing sexual, pornographic or illegal content, or material which is offensive in any way must not be viewed or download deliberately. Anyone who accesses such material inadvertently should exit the website immediately and contact Business Stream's IT Helpdesk with details of the website address. Business Stream IT Helpdesk will take steps to block this website to prevent this from happening again.

Limited and responsible personal use of the company internet service is permitted, subject to the control of line management.

Business Stream's IT service provider runs content checking software on the Internet service. This blocks access to inappropriate or high-risk websites. Users must not try to circumvent this service. If there is a legitimate business requirement for access to a blocked website then the Business Stream's IT Helpdesk can assist with the request.

Business Stream reserves the right to monitor device and user-based Internet activity for the purposes of security analysis, threat management and performance checks.

5. Communications

Business Stream is ultimately responsible for all business communications but will, as far as possible and appropriate, respect privacy and autonomy while working. Business Stream may monitor communications for reasons which include:

- providing evidence of business transactions
- ensuring that Business Stream's business processes, policies and contracts with staff and outsourced service providers are adhered to
- complying with any legal obligations
- monitoring standards of service, staff performance, and for staff training
- preventing or detecting unauthorised use of Business Stream's communications systems or criminal activities

- maintaining the effective operation of Business Stream's communication systems

Business Stream monitor telephone, email, instant messaging and internet traffic. Attributes monitored include sender, receiver, subject, attachments to e-mail, numbers called and duration of calls; addresses of websites visited, duration of visits, and files downloaded from the internet.

Sometimes it is necessary for Business Stream to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of HR.

In certain circumstances we may, subject to compliance with any legal requirements, access emails marked PERSONAL or in a folder marked PERSONAL. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be a breach of a contract with Business Stream.

It is important to use the correct medium of communication when sharing information. Sensitive information should only be shared using mediums that guarantee the secure delivery or storage of the data being transferred.

For guidance, some examples are given below:

- Do not disclose passwords via email, unless a secure email service is used
- Do not leave sensitive information on third party voicemail systems

6. Data Protection

Computer users must follow each of these principles:

- Data should only identify an individual where strictly necessary for the purpose of the task being performed.
- Personal data should not be disclosed where there is an indication that such data might be used for marketing products or services.
- If data is held about a number of individuals who are in dispute, no data about one individual should be disclosed to other parties without that individual's specific consent.
- Data should be adequate, relevant and not excessive, should be accurate and kept up to date,
- Data should not be kept for longer than is necessary.
- Data should be protected by adequate security measures.

This is not an exhaustive list of the data protection principles which must be followed. The Senior Compliance and Regulation Manager will issue further detailed guidance from time to time on the requirements of the Data Protection Act, and all employees will be required to comply with any such guidance.

7. Information Storage, Classification and Disposal

All information relating to our customers and business operations is confidential or restricted to a specific audience unless classified for public consumption.

All information that is stored, whether electronically or in paper form should have an appropriate data classification mark. Any information that is unmarked, is, by default, considered confidential. Data classification is especially important where information is being released in response to a Freedom of Information request. The Data Classification Policy or the Senior Compliance and Regulation Manager should be referenced for further information.

Care should be taken when storing information electronically, to ensure that data can only be viewed, changed or copied by authorised personnel. Only approved network shares, collaboration & communication systems or file sharing technologies should be used to store and share information. The Head of IT can provide further information or clarification on approved systems.

All information, including paper-based information, should be stored securely. Information should not be left unsecured when not in use. Confidential information should be stored securely or disposed of when no longer required. Hardcopy information should be disposed of using the secure shredding facilities provided. Consult with the Facilities Manager for more information on disposal of hardcopy. The Head of IT can advise further on how to dispose of electronic information securely.

8. Backups

Business data must be backed up and stored safely and securely, as advised and agreed by Business Stream IT team. Business data stored on the provided network drives or collaboration sites is regularly backed up by Business Stream IT function. Users are responsible for data held on local drives such as the C: drive and it should be backed up separately. Business Stream's IT Helpdesk can advise on how best to back up local data.

9. Passwords

Each employee, contractor, secondee, consultant, agency staff or nominated staff of outsourced service providers are accountable for any actions logged by their username on Business Stream's information technology and communications facilities. They must comply with the following:

- Do not share system usernames or passwords
- Passwords must be kept secure and confidential
- Do not write passwords down
- Do not base a password on any of the following:
    - anything obvious e.g. football teams
    - telephone numbers
    - car registrations
    - user, group or system identifiers, family names or company names or initials

Passwords should be changed every 60 days.

Passwords should have the following characteristics:

- Contain both upper and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-
- =\`{}[]:";'<>?,./)
- Are at least 12 alphanumeric characters long
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Authorised users must NOT:

- Reveal a password over the phone to anyone
- Talk about a password in front of others
- Hint at the format of a password (e.g., "my family name")
- Reveal a password on questionnaires or security forms
- Share a password with family members

- Reveal a password to colleagues whilst on annual leave
- Save a password in clear text in a file on a computer system

If an account or password is suspected to have been compromised it must be reported to the IT Helpdesk immediately.

10. Everyone's responsibility

All security incidents, both actual and suspected, must be reported immediately to a line manager or to Business Stream's IT Helpdesk. Outsourced service providers must report such instances to Business Stream's IT Helpdesk.