SB SKILLS SOLUTIONS
Information Security Policy (ISP)

This Policy should be read in conjunction with other Data Management and Information Governance Policies and related Codes of Practice (CoPs) including:
Information and Data Governance Framework (IDGF)
Data Protection Policy (DPP)
GDPR & Data Processing Policy & Practice (GDPR)
Information Security Policy (ISP)
Codes of Practice D1 > D14
CoP D1 Handling Personal Data
CoP D2 Access to Personal Data
CoP D3 Data Asset Register
CoP D4 Impact Assessment
CoP D5 Electronic Messaging
CoP D6 Password Policy
CoP D7 Inspection of Electronic Data
CoP D8 Clear desk & Screen Policy
CoP D9 Archiving
CoP D10 Media Classification
CoP D11 File Control
CoP D12 Shredding and Disposal
CoP D13 Equipment
CoP D14 Auditing
Privacy Notices
Student Privacy Notice
Website Usage Privacy Notice
Employee Privacy Notice

Compliance & IT Manager (CIM) - Steve Maddocks
Tel: 01695 558420
Email: steve@sbskills.co.uk
or
Senior Information and Risk Officer and Senior Data Protection Officer
Neil Beaumont, Director
Email: neil@sbskills.co.uk

Contents:

Information Security Policy (ISP)

1. Objectives

Information plays a fundamental role in supporting all activities of the Company. Properly securing all information that the Company processes is essential to the success of all its delivery, services, training and administrative activities. This is to be achieved through managing the three essential attributes of information security: confidentiality, integrity and availability, which are the vital building blocks for safeguarding the Company's information.

The objectives of this policy are to:

- enable adequate protection of all of the Company's information assets against loss, misuse or abuse;
- make all users aware of this policy and all associated policies, codes of practice and guidelines;
- make all users aware of the relevant UK and European Community legislation, and their responsibilities in regard to these;
- create an awareness that appropriate security measures must be implemented across the Company as part of the effective operation and support of information security;
- make all users understand their responsibilities for protecting the confidentiality, integrity and availability of the data they handle.

This Policy should be read in conjunction with the Company's **Data Protection Policy**, **GDPR and Data Processing Policy** and associated **Codes of Practice**, which provide more detailed guidance on protecting personal data and information security.

2. Scope

All Company staff, students and other authorised third parties including guests to Company, who may have access to information held by or on behalf of the Company, must adhere to the Company's Information Security Policy and its associated Codes of Practice. The scope of the policy covers their use of Company-owned/leased/rented and on-loan facilities, and all non-Company systems, owned/leased/rented/on-loan, when connected to the Company network directly or indirectly, to all Company-owned/licensed data and software, be they on Company or on non-Company systems, and to all data and software provided to Company by sponsors or external agencies.

The policy applies to all data held by the Company whether in electronic or physical format including by way of example:

- electronic data stored on and processed by fixed and portable computers and storage devices;
- data transmitted on networks;
- information sent by fax or similar transfer methods;
- all paper records;
- microfiche, visual and photographic materials including slides and CCTV;
- spoken, including face-to-face, voicemail and recorded conversation.

The Company's data can broadly be classified as personal data and non-personal data:

Personal data is treated in accordance with the Company's Data Protection and GDPR and Data Processing Policies and is afforded the highest standard of protection;

Non-personal data can include:

- sensitive organisational data such as commercially sensitive planning data and data protected by confidentiality agreements or legally privileged information – all of these categories of data are also afforded a high level of protection; and
- other organisational data that is either already made public (e.g. on the Company website) or is potentially disclosable to the public (e.g. pursuant to a request under the Freedom of Information Act) – such data must be accurate, must be kept up-to-date and must be protected from destruction and unauthorised interference.

The policy applies throughout the lifecycle of all information from creation, storage, and use to disposal.

Although the use of social media resources by Company members is unrestricted and not centrally moderated, the Company requires its members to ensure they respect this policy and cause no damage to the Company's reputation.

Security Awareness

The policies and procedures outlined below are incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors as follows:

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (Appendix A) before they commence their employment with the Company.
- Company security policies are reviewed annually and updated as needed.

3. Responsibilities

The key roles and responsibilities at Company with respect to data protection, GDPR and information governance/security and compliance with this policy are:

Senior Information Risk officer and Data Protection Officer (SIRO & DPO), supported by the **Compliance & ICT Manager (CIM)** and **Senior Management Team,** is responsible for informing and advising the Company and its staff on its information security and data protection obligations, and for monitoring compliance with those obligations and with the Company's policies alongside the management of Information Assets;

Compliance and ICT Manager (CIM) is the main information officer and is responsible for overseeing ICT's resources to manage day-to-day information security activities, and service desk. The CIM may decide to audit systems to identify and mitigate risks, or to make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

Duties include:

- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures.

The CIT department shall maintain daily administrative and technical operational security procedures (for example, user account maintenance procedures, and log review procedures). CIM and IT Response Team/Service Desk other system administrators shall:

- monitor and analyse security alerts and information and distribute to appropriate personnel.
- administer user accounts and manage authentication.
- monitor and control all access to data.

Head of Departments and Heads of Divisions (HODs) are responsible that staff, students and other authorised individuals within their department or division are informed, and comply with this policy, particularly section 11: Conditions of Use of IT Resources, and associated Codes of Practice. They are also responsible that all information assets held by their departments or divisions are included in the Company's Information Asset Register and an Information Asset Owner is assigned for every information asset.

Information Asset Owners are the assigned owners of Company information assets as listed in the Company's Information Asset Register managed and monitored by the SIRO. They are responsible for assessing information security and privacy risks annually for their assets and implementing appropriate measures accordingly as instructed by the SIRO.

The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

Facilitating participation upon hire and at least annually.

Ensuring that employees acknowledge in writing annually that they have read and understand all the Company's policies and CoPs.

Staff, Students and Authorised Third Parties must adhere to this and associated Codes of Practice. Compliance with the policy forms part of the Core Terms and Conditions of Service for Company staff and forms part of the Regulations for Students/learners. Section 11 of this policy, "**Conditions of Use of IT Resources (Acceptable Use Policy)**" is displayed and must be accepted by all staff and students before they can start using their Company user-name. Any actual, or suspected, information security incidents (such as accidental exposure or loss, unauthorised access, computer virus, malicious software) must be reported to the ICT's Service Desk immediately. Concerned individuals may contact any members of ICT or the CIM directly.

4. Acceptable Use Policy (Conditions of Use of IT Resources)

Any person using Company IT resources (referred to as a “user”) agrees and accepts that:

- Company IT resources are all hardware, software, services and resources made available for the Company business. They include all computer networks, wired or wireless, computers, printers, mobile devices, storage, audio visual systems, and associated information services including Cloud services;
- He/she must understand and abide by the advice provided and must enrol and complete the Company’s Information Security Awareness training;
- Use of Company IT resources, and their use to access non-Company IT resources, must be for the purpose of Company research, teaching, coursework, associated administration or other authorised use. No private commercial work is permitted without prior authorisation;
- Company business should be conducted only on information services provided by the Company. Using non-Company information services to carry out Company business puts Company data at risk and therefore is not allowed except with sufficient justification;
- Reasonable personal use of Company IT resources is permitted provided such use does not disrupt the conduct of Company business or other users;
- It is not permitted to connect active network devices such as network switches, hubs, wireless access points and routers to the Company network. All IP addresses will be allocated and administered only by ICT;
- He/she may not grant access to Company computing services to non-Company staff or students except where expressly permitted to do so in writing;
- When using Company IT resources the user must comply with the Company’s Information Security Policy and Acceptable Use Policy, and all relevant statutory and other provisions, regulations, rules and codes of practice. Specifically, but not exclusively, the user must:
    - not disclose to others their Company password and must understand and abide by code of practice for passwords;
    - not access or attempt to access IT resources at Company or elsewhere for which permission has not been granted or facilitate such unauthorised access by others;
    - not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any IT resources at the Company or elsewhere, e.g. port scanning;
    - not display, store, receive or transmit images or text which could be considered offensive or which is likely to bring the Company into disrepute, e.g. material of a pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory, illegal, discriminatory, or terrorist nature;

  - not forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' email, must not impersonate others in electronic communication and generate junk or offensive communications and must understand and abide by code of practice for electronic messaging;
  - ensure all mobile devices they access Company resources with are encrypted by an appropriate encryption software, and pin or password protected;
  - respect the copyright of all material and software made available by the Company and third parties and not use, download, copy, store or supply copyrighted materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the Company;
  - respect the copyright of all material and software made available by the Company and third parties and not use, download, copy, store or supply copyrighted materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the Company;
  - when holding data about living individuals, abide by the Company's Data Protection Policy DPP, to process information (that is, collect, use, share and dispose of) in accordance with the Principles of the data protection legislation. Students must not keep personal data concerning individuals in connection with their training without the express approval from their Head of Department;
  - when responsible for information assets as an identified Information Asset Owner, understand and abide by their responsibilities as defined in Code of Practice D3 and D4;
  - be aware that all information assets created/owned/stored by the user on or connected to Company IT resources may, in the instance of suspected wrong-doing, be subjected to inspection by Company or by statutory authorities. Should the information be encrypted the user shall be required to and must provide the decryption key;
  - establish what the terms of the licence are for any material and software which he/she uses through any platform and must not breach such licences including those which relate to "walk-in" access to particular materials which should only be accessed in SB Skills Solutions premises;

- As provided by the "Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000", made under the "Regulation of Investigatory Powers Act 2000" and "Prevent Duty Guidance" as directed by the "Counter-Terrorism and Security Act 2015" the Company will intercept and monitor electronic communications for the purposes permitted under those Regulations in accordance with Code of Practice D7;
- In the event of a suspected or actual information security incident or an unacceptable network event, the CIM may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network;

- In the event of further examination required, ICT may take action to examine any systems on the Company network by express permission from the SIRO;
- Other than as per any applicable statutory obligation, the Company will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT resource provided and/or managed by the Company;
- Whilst the Company takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data;
- Users' name, address, photograph, status, e-mail name, login name, alias, Company Identifier (CID) and other related information will be stored in computerised form for use for administrative and other purposes e.g. monitoring system usage;
- These conditions apply to non-Company owned equipment e.g. personal Laptops, home PCs when connected to the Company network, directly and/or via a VPN, for the duration that the equipment is using the Company network;
- Breach of these conditions may lead to Company disciplinary procedures being invoked, with penalties which could include suspension from the use of all Company IT resources for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the Company and may involve civil or criminal action being taken against the user;
- If you have any questions, contact ICT's Service Desk or CIM;
- All guests using Company IT facilities and/or the Company internet connection must be known to a member of Company as their sponsor. Sponsors must be able to identify and take responsibility for the actions of their individual guests.

5. Company Information Asset Register and Data Impact Assessment

- The Company maintains an Information Asset Register that contains the details of information assets used in Company. It is the responsibility of Heads of Departments and Divisions reporting to the SIRO/DPO to assign Information Asset Owners for every information asset kept by their departments and record these in the Information Asset Register (CoP D3).
- A data privacy impact assessment must be carried out for all existing information assets annually. A data privacy impact assessment must also be carried out for all new information assets at the time of inception. For the ones identified as containing sensitive data, measures to mitigate those risks must be agreed, implemented and also included in the asset register. It is the responsibility of the Heads of Departments to review their Information Assets annually (CoP D4).

6. Physical Security

Security Perimeters

- SB Skills Solutions ensure that Security perimeters (barriers such as walls, fob-controlled entry gates/doors or manned reception desks) are used to protect areas that contain information and information processing facilities.
- Security perimeters are clearly defined, and the siting and strength of each of the perimeters is dependent on the security requirements of the assets within the perimeter and have been arrived at because of a formal risk assessment;
- Perimeters of buildings containing information processing facilities are physically sound; the external walls of the site are of solid construction and all external fob-entry doors are suitably protected against unauthorized access with control mechanisms, e.g., bars, alarms, locks etc.; doors and windows are locked when unattended and external protection is implemented for windows, particularly at ground level;
- Manned reception area and other means to control physical access to the site or building is in place; access to sites and buildings is restricted to authorized personnel only;
- All fire doors on a security perimeter are alarmed and monitored; and suitable intruder detection systems are installed and regularly tested to cover all external doors and accessible windows.

Entry Controls

- Secure areas are protected by appropriate fob-entry controls to ensure that only authorised personnel are allowed access.
- Date and time of entry and departure of visitors is recorded, and all visitors are supervised unless their access has been previously approved; they are granted access for specific, authorized purposes and are issued with instructions on the security requirements of the area and on emergency procedures;
- Access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only;
- All employees, contractors and third party users and all visitors are required to wear visible identification and are trained to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
- third party support service personnel are granted restricted access to secure areas or sensitive information processing facilities only when required; this access is supervised and monitored;
- access rights to secure areas are regularly reviewed and updated and revoked when necessary.

Protection against Threats

- Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster are designed and applied.
- SB Skills Solutions ensures that risk assessments are undertaken to ensure that relevant countermeasures against external and environmental threats are identified.

- Where SB Skills Solutions outsource data hosting, we take steps to ensure that physical security requirements are contractually enforced in-line with the requirements of ISO 27001.
- Should SB Skills Solutions be required to lease property, the company shall maintain contact with relevant Landlords for its UK sites to ensure that adequate countermeasures are in place commensurate with the level of risk.

Working in Secure Areas

- SB Skills Solutions ensure that physical protection and guidelines for working in secure areas are designed and applied.
- unsupervised working in secure areas is avoided both for safety reasons and to prevent opportunities for malicious activities;
- vacant secure areas are physically locked and periodically checked; and,
- photographic, video, audio, or other recording equipment, such as cameras in mobile devices, are not allowed, unless authorized.

Access, Delivery and Loading

- SB Skills Solutions ensures that access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

7. Equipment Security

- SB Skills Solutions ensure that equipment is protected from physical and environmental threats.
- Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage.
- Equipment security shall be the joint responsibility of the SIRO/DPO and the Asset Owners within the Company.

Equipment Siting and Protection

- Equipment are sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
- The following guidelines will be applied to all sites and risk assessments will be reassessed at least annually.
- equipment is sited to minimize unnecessary access into work areas;
- information processing facilities handling sensitive data are positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;
- items requiring special protection are isolated to reduce the general level of protection required;
- controls are adopted to minimize the risk of potential physical threats, e.g., theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;
- guidelines for eating, drinking, and smoking in proximity to information processing facilities are established; and,

- environmental conditions, such as temperature and humidity, are monitored for conditions which could adversely affect the operation of information processing facilities.

Supporting Utilities

- Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
- All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air-conditioning are designed to be adequate for the systems they are supporting.
- Support utilities are regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.
- Where deemed appropriate by risk assessment fallback network provisions, UPS, laptops which can operate on their own power and 3G data cards have been deployed.

Cabling Security

- Power and telecommunications cabling carrying data or supporting information services are protected from interception or damage.
- All cables used to facilitate the use of equipment are adequately protected for their type and usage, and meet industry standard, and equipment manufacturer specifications / recommendations for each use type.

Equipment Maintenance

- SB Skills Solutions ensure that all applicable equipment is maintained.
- equipment is maintained in accordance with the supplier’s recommended service intervals and specifications; and,
- only authorized maintenance personnel carry out repairs and service equipment;

Security of Equipment off-premises

- SB Skills Solutions ensure that security is applied to off-site equipment taking into account the different risks of working outside the Company’s premises.
- regardless of ownership, the use of any information processing equipment outside the Company’s premises must be authorized by management.
- the following guidelines shall be considered for the protection of off-site equipment:
- equipment and media taken off the premises should not be left unattended in public places; portable computers should be carried as hand luggage and disguised where possible when travelling;
- manufacturers’ instructions for protecting equipment should be always observed e.g. protection against exposure to strong electromagnetic fields;
- home-working procedures are determined by a risk assessment and suitable controls applied as appropriate e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office; and adequate insurance cover is in place to protect equipment off-site.
- security risks, e.g. of damage, theft, or eavesdropping, may vary considerably between locations and are considered in determining the most appropriate controls.

- information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper, or other media which is held for home working or being transported away from the normal work location.
- Where necessary laptops shall be protected by PGP Whole Disk Encryption to protect data at rest.

Secure Disposal or Re-use of Equipment

- All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
- All disposals from the Information Systems environment are controlled via the Change Management System, to provide an audit trail. Assets will not be offered to you for purchase.
- Where outsourced service providers are responsible for the disposal of assets, procedures shall be in place to ensure that:
    - All software is uninstalled
    - Information on any computer media is destroyed or disposed of under conditions which prevent casual or willful access by unauthorized people.
    - ICT secure wipe all PCs and Laptops before re-issue or before disposal using a recognized technique (DBAN).

Removal of Property

- Staff are aware of their responsibilities for handling removable media. If are unsure, you should ask ICT service desk to ensure that removable media is treated correctly.
- The use of removable media to store any learner information is prohibited.
- Staff must not store any information about your clients however disseminated or presented on removable media.
- Information, statistics, or data held on removable media that relates to learners to be used for presentations or meetings must be de-personalised. Staff should remove any personal information such as date of birth, name, address, telephone number, NI number and so on.
- Staff are prohibited from storing company sensitive information or company employee information on removable media.
- extreme caution should be used when accepting removable media from third parties such as learners or external organisations. Many viruses are passed using floppy disks for example. You must consult with ICT before accepting and using such removable media.
- Removable media is defined as (but not limited to) floppy disks, cd, DVD, flash memory and USB memory.
- equipment, information, or software should not be taken off-site without prior authorization;
- employees, contractors and third party users who have authority to permit off-site removal of assets should be clearly identified;
- time limits for equipment removal should be set and returns checked for compliance; and,

- where necessary and appropriate, equipment should be recorded as being removed off-site and recorded when returned.
- Spot checks, undertaken to detect unauthorized removal of property, may also be performed to detect unauthorized recording devices, etc., and prevent their entry into the site. Such spot checks should be carried out in accordance with relevant legislation and regulations. Individuals should be made aware is spot checks are carried out, and the checks shall only be performed with authorization appropriate for the legal and regulatory requirements

8. Employment Security

Security roles and responsibilities, as laid down in this policy and related Codes of Practice, should be included in job descriptions, where appropriate. These should include any general responsibilities for implementing the security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

Screening

Each person requiring access to this information is including employees, contractors and external party personnel are required to adhere to the Staff Vetting Procedures, which include:

- Identity;
- Nationality and Immigration Status;
- Employment History (for a minimum of the past 3 years); and
- Criminal Records Bureau checks.

References will be sought as required.

As part of their contractual obligation, employees, contractors and third party users agree and sign the terms and conditions of their employment or other contract.

During employment. Attention is drawn to the SB Skills Solutions Staff Handbook.

Management Responsibilities

The SMT and HoDs within SB Skills Solutions require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation which meet the standards of rigour required.

Management ensure that personnel be made aware of their security obligations on induction and regularly thereafter through scheduled refresher and up-date training This training shall be supported by their agreement to this Information Security Policy and regular updates are provided weekly via emails to all staff; e-learning module updates and the SB Skills Solutions intranet pages.

Disciplinary Process

SB Skills Solutions have implemented a formal disciplinary process for employees who have committed a security breach.

The Company’s aim is to ensure that there will be a fair and consistent approach to the enforcement of standards of conduct and performance throughout the organisation. We are committed to providing our people with appropriate training, coaching, mentoring, guidance, supervision and support to enable them to achieve personal and corporate objectives.

This policy and procedure are designed to help and encourage all individuals to achieve and maintain standards of conduct, attendance and job performance. The policy is available to all our people and a précis of the policy is available in the SB Skills Solutions Staff Handbook.

The policy aims to ensure matters are dealt with quickly and individuals are given every opportunity to improve.

Termination or Change of employment

Responsibility for performing employment termination or change of employment rests with The Company's HR department.

The Company's HR department have produced relevant procedures to manage the termination or change of employment of staff. A précis of these procedures is available in the SB Skills Solutions Staff Handbook.

Return of Assets

All employees, contractors and third parties sign a contract that requires them to return all of the organisation's assets in their possession upon termination of their employment, contract or agreement. Information on the assets held by the individual is held in a separate asset register.

You must return your mobile phone (including power supply and cables and other parts) to your Line Manager or appropriate supervisor if you leave our employment. If you do not return all parts of your mobile telephone, we may charge you for the costs of those parts.

A précis of these procedures is available in the SB Skills Solutions Staff Handbook.

Removal of Access Rights

The access rights of all SB Skills Solutions employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon any change in the role or responsibility of the employee.

HR and the IT Service Desk ensure that the system access rights of all employees, contractors and third parties are removed upon termination of their employment, contract or agreement or adjusted upon change of duties.

9. Information Access and Privilege Controls

An Information access control policy is established, documented, and reviewed based on business and security requirements for information access.

The policy takes account of the following:

- Security requirements of individual business applications;
- Identification of all information related to the business applications and the risks the information is facing;
- Policies for information dissemination and authorization, e.g.the need to know principle and security levels and classification of information;
- Consistency between the access control and information classification policies of different systems and networks;
- Relevant legislation and any contractual obligations regarding protection of access to data or services;
- Standard user access profiles for common job roles in the organization;
- Management of access rights in a distributed and networked environment which recognizes all types of connections available;
- Segregation of access control roles, e.g., access request, access authorization, access administration;
- Requirements for formal authorization of access requests;
- Requirements for periodic review of access controls;
- Removal of access rights;

User Access Management

- Access is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- Checking that the user has authorization from the asset owner for the use of the information system or service;
- Checking that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy,
- Giving users a written statement of their access rights;
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to data.
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:
- Name of person making request:
- Job title of the newcomers and workgroup:
- Start date:
- Services required (default services are: MS Outlook, MS Office and Internet access):
- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all company systems is provided by IT and can only be started after proper procedures are completed.
- Maintaining a formal record of all persons registered to use the service.
- Immediately removing or blocking access rights of users who have changed roles or jobs or left the organization.
- Periodically checking for, and removing or blocking, redundant user IDs and accounts - Ensuring that redundant user IDs are not issued to other users.
- As soon as an individual leaves the Company employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

Access and Privilege Control Policy

Access Control systems are in place to protect the interests of all users of Company computer systems by providing a safe, secure and readily accessible environment in which to work.

The Company will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.

- Generic or group IDs shall not normally be permitted but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users are obligated to report instances of non-compliance to the Company SIRO or CIM.
- Access to The Company IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any The Company IT resources and services will be provided without prior authentication and authorization of a user's the Company Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by The Company policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods, as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights

Review of User Access Rights

The Company shall review users' access rights at regular intervals using a formal process. The review of access rights shall consider the following guidelines:

- Users' access rights will be reviewed at regular intervals, e.g.a period of 3 months, and after any changes, such as promotion, demotion, or termination of employment;
- User access rights shall be reviewed and re-allocated when moving from one employment to another within the same organization;
- Authorizations for special privileged access rights shall be reviewed at more frequent intervals, e.g.at a period of 3 months;
- Privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained; and,
- Changes to privileged accounts shall be logged for periodic review.

10. User Password Management

Users shall be issued with a user account and password from the ICT Service Desk after line Manager approval. Users must not share this with anyone. It is the user responsibility to ensure that their password remains secure.

- Users are required to sign a statement to keep personal passwords confidential. This signed statement is included in the terms and conditions of employment
- Line Managers have a specific responsibility to ensure that employees do not disclose their password or share it between colleagues. Line Managers are responsible for informing the ICT Service Desk of whenever someone leaves so that their user account can be disabled.
- You are required by the system to change your password every 28 days. When your password expires, you will be required to choose a password that is: Minimum 8 characters; Includes at least 1 number and a capital letter (e.g.Abcde123); You will not be able to choose the same password for 8 changes.
- If you try to log in with the wrong password, you will be locked out permanently after 3 failed attempts and will need to contact an IT Administrator to reset it.

11. Operational Security Procedures

The Company shall ensure that documented procedures are prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures specify the instructions for the detailed execution of each job including:

- Processing and handling of information;
- Back-up rules and guidelines;
- Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;

- Support contacts in the event of unexpected operational or technical difficulties;
- Special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;
- System restart and recovery procedures for use in the event of system failure;
- The management of audit-trail and system log information.

Operating procedures, and the documented procedures for system activities, are treated as formal documents and changes authorized by senior management. Where technically feasible, information systems are managed consistently, using the same procedures, tools, and utilities.

The Company shall ensure that all relevant operating procedures are published on the Company intranet site.

Change Management

All major changes to system hardware, software, configuration, authorised users and operating procedures are to be authorised.

All security relevant changes supported by a sound business justification are considered and those approved are actioned and recorded in the configuration documentation.

- Identification and recording of significant changes;
- Planning and testing of changes;
- Assessment of the potential impacts, including security impacts, of such changes;
- Formal approval procedure for proposed changes;
- Communication of change details to all relevant persons; and,
- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Formal management responsibilities and procedures are in place to ensure satisfactory control of all changes to equipment, software, or procedures. When changes are made, an audit log containing all relevant information is retained.

Segregation of Duties/Separation of Development, Test and Operational:

The Company shall ensure that duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation’s assets.

The Company shall maintain a separate development system strictly under the control of the IT Department.

The Company shall implement and operate a three-phase development approach involving a dedicated development environment, progressing to a separate user acceptance testing environment and an operational environment. Each of these stages is segregated from each other.

- Rules for the transfer of software from development to operational status are defined and documented;
- Development and operational software run on different systems or computer processors and in different domains or directories;
- Compilers, editors, and other development tools or system utilities are not be accessible from operational systems when not required;

- The test system environment emulates the operational system environment as closely as possible;
- Users have different user profiles for operational and test systems, and menus display appropriate identification messages to reduce the risk of error;
- Sensitive data must not be copied into the test system environment.

Third Party Service Delivery Management

The Company shall ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Monitoring and review of third party services shall ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly. This should involve a service management relationship and process between the organization and the third party to:

- Monitor service performance levels to check adherence to the agreements;
- Review service reports produced by the third party and arrange regular progress meetings as required by the agreements;
- Provide information about information security incidents and review of this information by the third party and the organization as required by the agreements and any supporting guidelines and procedures;
- Review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered; and,
- resolve and manage any identified problems.

The responsibility for managing the relationship with a third party shall be assigned to a designated individual or service management team within the Company. In addition, we shall ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed. We should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed, or managed by a third party.

The Company shall ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response through a clearly defined reporting process, format and structure.

Managing Changes to Third Party Services

The Company shall ensure that changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

The process of managing changes to a third party service shall take account of:

Changes made by the Company to implement:

- enhancements to the current services offered;
- development of any new applications and systems;

- modifications or updates of the Company's policies and procedures;
- new controls to resolve information security incidents and to improve security;

Changes in third party services to implement:

- changes and enhancement to networks;
- use of new technologies;
- adoption of new products or newer versions/releases;
- new development tools and environments;
- changes to physical location of service facilities;

System Planning and Acceptance

- The Company shall ensure that the use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
- For each new and ongoing activity, capacity requirements are identified. System tuning and monitoring is applied to ensure and, where necessary, improve the availability and efficiency of systems.
- Detection controls have been put in place to indicate problems in due time. Projections of future capacity requirements take account of new business and system requirements and current and projected trends in the Company's information processing capabilities.
- Particular attention is paid to any resources with long procurement lead times or high costs. They identify trends in usage, particularly in relation to business applications or management information system tools.
- Managers use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services and plan appropriate action.

The following items are considered prior to formal acceptance of new systems:

- Performance and computer capacity requirements;
- Error recovery and restart procedures, and contingency plans;
- Preparation and testing of routine operating procedures to defined standards;
- Agreed set of security controls in place;
- Effective manual procedures;
- Business continuity arrangements;
- Evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;
- Evidence that consideration has been given to the effect the new system has on the overall security of the organization;
- Training in the operation or use of new systems; and,
- Ease of use, as this affects user performance and avoids human error.

For major new developments, the operations function and users are be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design.

12. Anti-Virus and Malicious Code Controls

SB Skills Solutions Information Systems are protected against virus attack using tools that are routinely maintained. These are deployed and updated to all machines connected to the network including those connected by dial-up. All removable media, email and Internet downloads supplied by us are virus scanned prior to use.

Equipment not connected to the network is excluded from this arrangement and you must make alternative arrangements with us for this to be scanned.

The systems on which the information software applications reside have McAfee VirusScan Enterprise, VirusScan for NetApp and Group-Shield for Exchange as required to protect against infection by malicious software.

- All machines must be configured to run the latest anti-virus software as approved by SB Skills Solutions Ltd;
- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits);
- All removable media (for example floppy and others) should be scanned for viruses before being used;
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement of 3 months online and 1 year offline;
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans;
- End users must not be able to modify and any settings or alter the antivirus software;
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

The Company ensures that all mobile code has to carry a valid Microsoft Digital Certificate before it is executed. Only mobile code that can be executed will be one which carries a valid digital certificate, users will not be able to accept or reject the execution of mobile code.

13. Information Handling and Exchange Procedures

Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.

The following shall be considered to assist in handling, processing, storing, and communicating information consistent with its classification:

- All media will be handled and labeled in accordance with its indicated classification level;
- Access restrictions to prevent access from unauthorized personnel;
- Maintenance of a formal record of the authorized recipients of data;
- Ensuring that input data is complete, that processing is properly completed, and that output validation is applied;
- Protection of spooled data awaiting output to a level consistent with its sensitivity;
- Storage of media in accordance with manufacturers' specifications;
- Keeping the distribution of data to a minimum;
- Clear marking of all copies of media for the attention of the authorized recipient; and,
- Review of distribution lists and lists of authorized recipients at regular intervals.

Security of system documentation: SB Skills Solutions shall ensure that access to systems documentation is controlled and limited to those people with the appropriate clearance who have need to access the system documentation.

Information exchange policies and procedures:

- SB Skills Solutions shall ensure that formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
- Where client Information or software that is used or exchanged, electronically or physically, the information must be protected to ensure the Confidentiality and Integrity and Availability of the information or software.

Exchange agreements - Agreements shall be established for the exchange of information and software between the organisation and external parties. Exchange agreements shall consider the following security conditions:

- Management responsibilities for controlling and notifying transmission, dispatch, and receipt;
- Procedures for notifying sender of transmission, dispatch, and receipt;
- Procedures to ensure traceability and non-repudiation;
- Minimum technical standards for packaging and transmission;
- Courier identification standards;
- Responsibilities and liabilities in the event of information security incidents, such as loss of data;
- Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected;
- Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations;
- Technical standards for recording and reading information and software;
- Any special controls that may be required to protect sensitive items, such as cryptographic keys.

Physical Media In Transit - Media containing information shall be protected against unauthorised access, misuse or corruption during transportation beyond Twin Group's physical boundaries.

- Reliable transport or couriers shall be used;
- A list of authorized couriers shall be agreed with management;
- Procedures to check the identification of couriers shall be developed;
- Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g., for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture, or electromagnetic fields;
- Controls shall be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification; examples include: use of locked containers; delivery by hand; tamper-evident packaging (which reveals any attempt to gain access); in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

14. Management & Disposal of Removable Media

SB Skills Solutions shall ensure that procedures are in place for the management of removable media. The following guidelines for the management of removable media shall be considered:

- If no longer required, the contents of any re-usable media that are to be removed from the organization shall be made unrecoverable;
- Where necessary and practical, authorization should be required for media removed from the organization and a record of such removals shall be kept maintaining an audit trail;
- All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications;
- Information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers' specifications) shall be also stored elsewhere to avoid information loss due to media deterioration;
- Registration of removable media shall be considered to limit the opportunity for data loss; and,
- Removable media drives shall only be enabled if there is a business reason for doing so.
- All procedures and authorization levels should be clearly documented.

SB Skills Solutions shall ensure that media shall be disposed of securely and safely when no longer required, using formal procedures.

- Media containing sensitive information shall be stored and disposed of securely and safely, e.g.by incineration or shredding, or erased of data for use by another application within the organization;
- Procedures are in place to identify the items that might require secure disposal;
- Disposal of sensitive items should be logged where possible in order to maintain an audit trail.
- When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of non-sensitive information to become sensitive.

15. Electronic Messaging

Client Information may only be transmitted by electronic messaging systems when measures appropriate to the sensitivity and/or Information Classification of the information have been taken and when due consideration has been given to the route by which the information will be sent to the recipient.

All email received must be scanned for malicious software and measures implemented to prevent such software infecting Information Systems and Services.

Security considerations for electronic messaging should include the following:

- Protecting messages from unauthorized access, modification, or denial of service;
- Ensuring correct addressing and transportation of the message;
- General reliability and availability of the service;
- Legal considerations, for example requirements for electronic signatures;
- Obtaining approval prior to using external public services such as instant messaging or file sharing;

- Stronger levels of authentication controlling access from publicly accessible networks.

When necessary The Company shall implement policies and procedures to protect information associated with the interconnection of business information systems.
On-line Transactions - The Company shall ensure that controls are applied to protect Systems or Services involved in electronic commerce from network threats. Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
The Company shall implement controls to protect Systems or Services involved in electronic commerce from network threats. The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification or unauthorized modification.

Monitoring Electronic Communications

In accordance with the "Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000", made under the "Regulation of Investigatory Powers Act 2000" (RIPA) 2000, the Company will exercise its right to intercept and monitor electronic communications received by and sent from the Company for the purposes permitted under those Regulations. The purposes cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to the system, e.g. hacking and denial of service attacks, ensuring the effectiveness of its operations and compliance with Company policies and regulations. The monitoring process will be carried out in accordance with Code of Practice D7.

Information Back-Up

- Data held within the IT infrastructure follows a strict security and backup regime to support data loss and disaster recovery.
- Staff are responsible for the integrity and security of any material retained locally on your machine or on removable media. You are not permitted to store any work related information or data (including learner or jobseeker information) locally on your machine or on removable media.
- All files (including those on the student server) are backed up nightly (Monday - Thursday), weekly (Friday) and monthly (at the end of month).
- In addition to this, files are archived quarterly and kept forever (so they are retrievable). This workload is shared across 2 hardware devices.

All backups are stored in a fire-resistant safe (2 hours) except for the "day-before-yesterday" backups which are taken off-site by the IT Administrator or another member of the IT team in his absence.

16. System Configuration and Network Security

SB Skills Solutions ensure that networks shall be adequately managed and controlled, to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. All users with access to Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The Company ensure that security features, service levels, and management requirements of all network services are identified and included in any network services agreement, whether these services are provided in-house or outsourced to third-party providers.

Network Access

- Users are only provided with access to the services that they have been specifically authorized to use;
- User authentication is required for all external connections and remote access systems;
- Automatic equipment identification is implemented to authenticate connections from specific locations and equipment;
- All diagnostic and configuration ports shall be closed and access to their use strictly controlled, being made available to IT Department staff only;
- Remote, physical, and logical access to diagnostic and configuration ports shall be physically controlled and are subject to controlled access;
- Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, shall be disabled, or removed;
- The Company shall implement a technical architecture across networks which ensures that groups of information services, users, and information systems are segregated on networks
- The Company shall ensure that the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications;
- The network access rights of users should be maintained and updated as required by the access control policy;
- Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications;
- The requirements for network routing control are based on the access control policy.

Network Security

- Firewalls are implemented at each internet connection and any demilitarized zone and the internal company network;
- A network diagram detailing all the inbound and outbound connections is maintained and reviewed every 6 months;
- A firewall and router configuration document are maintained which includes a documented list of services, protocols and ports including a business justification;
- Firewall and router configurations restrict connections between untrusted networks and any systems in the information environment;
- Stateful Firewall technology is implemented where the Internet enters the Company network to mitigate known and on-going threats;
- Firewalls are also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network;
- All inbound and outbound traffic is restricted to that which is required for the information environment;
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented;

- All outbound traffic is authorized by management (i.e. list of whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented;
- The Company has firewalls between any wireless networks and the information environment.;
- The Company quarantine wireless users into a DMZ, where they are authenticated and firewalled as if they were coming in from the Internet;
- Disclosure of private IP addresses to external entities must be authorized;
- A topology of the firewall environment is documented and has to be updated in accordance with the changes in the network;
- The firewall rules are reviewed on a six-month basis to ensure validity and the firewall has a clean-up rule at the bottom of the rule base;
- No direct connections from Internet to information environment will be permitted. All traffic has to traverse through a firewall.

System Configuration and Passwords

All users with access to Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- A system configuration standard has been developed along industry acceptable hardening standards (SANS, NIST, ISO);
- System configurations are updated as new issues are identified (as defined in PCI DSS);
- System configurations include common security parameter settings;
- The systems configuration standard is applied to any new systems configured;
- All default accounts and passwords for the systems must be changed at the time of provisioning the system/device into the Company network and all unnecessary services and user/system accounts are disabled;
- All unnecessary default accounts are removed or disabled before installing a system on the network.
- Security parameter settings must be set appropriately on System components;
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed;
- All unnecessary services, protocols, daemons etc., must be disabled if not in use by the system;
- Any insecure protocols, daemons, services in use must be documented and justified;
- All users with access to the network and information must have a unique ID;
- All users must use a password to access the company network or any other electronic resources;
- All user ID’s for terminated users must be deactivated or removed immediately;
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account;

- All system and user level passwords must be changed on at least a quarterly basis;
- A minimum password history of four must be implemented;
- A unique password must be setup for new users and the users prompted to change the password on first login;
- Shared or generic user account or password or other authentication methods must not be used to administer any system components;
- Where SNMP is used, the community strings are defined as something other than the standard defaults of "public," "private" and "system" and are different from the passwords used to log in interactively;
- All non-console administrative access uses appropriate technologies like ssh or vpn etc., or strong encryption is invoked before the administrator password is requested;
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands;
- Administrator access to web based management interfaces is encrypted using strong cryptography;
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

  Be as long as possible (never shorter than 6 characters).
  Include mixed-case letters, if possible.
  Include digits and punctuation marks, if possible.
  Not be based on any personal information.
  Not be based on any dictionary word, in any language.

If an operating system without security features is used then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program. To protect against network analysis attacks, both the workstation and server should be cryptographically secured with strong protocols such as encrypted Netware login and Kerberos.

17. Cryptographic Controls

A policy on the use of cryptographic controls for protection of information is implemented as follows:

- PGP encryption products have been selected as control of choice, commencing with whole disk encryption to laptops and the distribution of email encryption facilities to key users;
- Data at rest shall be protected by SQL Server 2008 configured in FIPS 140-2 compliant mode, using Transparent Data encryption;
- Edge sites shall be secured using Checkpoint VPN technology which including AES 256 bit key exchange using SHA1 to protect data integrity and IPSEC Phase 2 AES 128 bit encryption using MD5 to protect data integrity;
- Key management shall be in place to support the organization’s use of cryptographic techniques.
- SIRO and CIM have approved the use of cryptographic techniques to protect the confidentiality, authenticity, and integrity of Information;

- Cryptographic keys shall be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected;

The key management system is based on an agreed set of standards, procedures, and secure methods for:

- Generating keys for different cryptographic systems and different applications;
- Generating and obtaining public key certificates;
- Distributing keys to intended users, including how keys should be activated when received;
- Storing keys, including how authorized users obtain access to keys;
- Changing or updating keys including rules on when keys should be changed and how this will be done;

Dealing with compromised keys;

- Revoking keys including how keys should be withdrawn or deactivated, e.g., when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);
- Recovering keys that are lost or corrupted as part of business continuity management;
- Logging and auditing of key management related activities.

18. Technical Vulnerability Management and Patch Management

Timely information about technical vulnerabilities of information systems being used shall be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

All Company workstations and servers are patched to the latest level to protect the asset from known vulnerabilities.

The Systems Administrators review exposure lists daily to remain abreast of patch requirements and wherever possible all systems, software must have automatic updates enabled for system patches. Security patches must be installed within one month of release. Any exceptions to this process must be documented.

19. Wireless Policy

Installation or use of any wireless device or wireless network intended to be used to connect to any of the company networks or environments is prohibited.

A quarterly test should be run to discover any wireless access points connected to the company network

Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:

- Any devices which support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the CIM or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology it should be approved by the company and the following wireless standards have to be adhered to:

- Default SNMP community strings and passwords, passphrases, Encryption keys/security related defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the company.
- The firmware on the wireless devices has to be updated accordingly as per vendors release schedule
- The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
- Any other security related wireless defaults should be changed if applicable.

Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of company data.

An Inventory of authorized access points along with a business justification must be maintained.

20. Control Monitoring and Audit Logging

This procedure covers all logs generated for systems within the data environment, based on the flow of data over the Company network, including the following components:

- Operating System Logs (Event Logs and sub logs);
- Database Audit Logs;
- Firewalls & Network Switch Logs;
- IDS Logs;
- Antivirus Logs;
- CCTV Video recordings;
- File integrity monitoring system logs;

Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline. Review of logs is to be carried out by means of the Company's network monitoring system which is controlled from the Company console. The console is installed on the server located within the Company data centre environment.

The Company defines which individuals have a job-related need to view audit trails and access log files. The network monitoring system software is configured to alert the ICT Response Team to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to a dashboard browser-based interface, monitored by the ICT Response Team with Email/SMS alerts to the Team mailbox with a summary of the incident.

1.The following Operating System Events are configured for logging, and are monitored by the console:

- Any additions, modifications or deletions of user accounts;
- Any failed or unauthorised attempt at user logon;
- Any modification to system files;
- Any access to the server, or application running on the server;
- Actions taken by any individual with root or administrative privileges;
- Any user access to audit trails;

- Any creation / deletion of system-level objects installed by Windows.

2.The following Database System Events are configured for logging, and are monitored by the network monitoring system:

- Any failed user access attempts to log in to a database;
- Any login that has been added or removed as a database user to a database;
- Any login that has been added or removed from a role;
- Any database role that has been added or removed from a database;
- Any password that has been changed for an application role;
- Any database that has been created, altered, or dropped;
- Any database object, such as a schema, that has been connected to;
- Actions taken by any individual with privileges;

3.The following Firewall Events are configured for logging, and are monitored by the network monitoring system:

- ACL violations;
- Invalid user authentication attempts;
- Logon and actions taken by any individual using privileged accounts;
- Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified);

4.The following Switch Events are configured for logging and monitored by the network monitoring system:

- Invalid user authentication attempts;
- Logon and actions taken by any individual using privileged accounts;
- Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified);

5.The following Intrusion Detection Events are configured for logging, and are monitored by the network monitoring system:

- Any vulnerability listed in the Common Vulnerability Entry database;
- Any generic attack(s) not listed;
- Any known denial of service attack(s);
- Any traffic patterns that indicated pre-attack reconnaissance occurred;
- Any attempts to exploit security-related configuration errors;
- Any authentication failure(s) that might indicate an attack;
- Any traffic to or from a back-door program;
- Any traffic typical of known stealth attacks;

6.The following File Integrity Events are configured for logging and monitored by:

- Any modification to system files;
- Actions taken by any individual with Administrative privileges;
- Any user access to audit trails;
- Any Creation / Deletion of system-level objects installed by Windows;

For any suspicious event confirmed, the following must be recorded and the SIRO and company directors informed:

- User Identification/ID;
- Success or Failure indication;
- Event Origination (e.g. IP address);
- Reference to the data, system component or resource affected;
- Dates, times, and details of key events, e.g.log-on and log-off;

- Terminal identity or location if possible;
- Records of successful and rejected system access attempts;
- Records of successful and rejected data and other resource access attempts;
- Changes to system configuration;
- Use of privileges;
- Use of system utilities and applications;
- Files accessed and the kind of access;
- Network addresses and protocols;
- Alarms raised by the access control system; and,
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

Regularity of review of monitoring activities depends on the risks involved. Risk factors that should be considered include the:

- Criticality of the application processes;
- Value, sensitivity, and criticality of the information involved;
- Experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited;
- Extent of system interconnection (particularly public networks);
- Logging facility being de-activated.

Audit log information shall be kept secure and only made available to privileged staff with appropriate system authority.

Logs are protected against unauthorized changes and operational problems with the logging facility including:

- Alterations to the message types that are recorded;
- Log files being edited or deleted; and,
- Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

System administrator and system operator activities are also logged and reviewed. Active Directory is used to track these activities and system-wide events.

Logs shall include:

- The time at which an event (success or failure) occurred;
- Information about the event (e.g., files handled) or failure (e.g., error occurrence and corrective action taken);
- Which account and which administrator or operator was involved; and,
- Which processes were involved.

All faults shall be logged, analyzed and appropriate action taken.

There are processes for handling reported faults including:

- Review of fault logs to ensure that faults have been satisfactorily resolved;
- Review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

The Company maintains a full synchronized timing system throughout the whole of the network.

21. Penetration Testing Methodology

External intrusion tests will be performed remotely from the supplier's premises Internal intrusion tests will be conducted in the Company. Audit teams must have access to the organisation's network. It must manage access permissions to the building early enough to ensure that the audit team can access without problems during planning period.

All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.

If an incident occurs during the execution of the tests that has an impact on the systems or services of the organisation, the incident should be brought immediately to the attention of those responsible for incident management in the project

Technical tests must follow the OSSTMM methodology. Tests must be conducted at network, system and application level and must ensure they identify any vulnerabilities:Injections; Buffer overflows; Insecure storage of cryptographic keys; Insecure Communications; Improper error handling; Cross -site scripting (XSS); Control of inappropriate access; Cross - site request forgery (CSRF); Broken authentication and incorrectly session management; and any other vulnerability considered High Risk by the organization.

For all findings or vulnerabilities identified during the tests carried out, documented sufficient evidence to prove the existence of the same must be provided. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.

As a result of tests performed should generate a document containing at least the following sections: Introduction, Executive Summary, Methodology, Identified vulnerabilities, Recommendations for correcting vulnerabilities, Conclusions, and Evidence.

22. Incident Response Planning and Implementation

All staff have a responsibility to recognize and to make known to the appropriate authority, all Security Incidents and any information which indicates a security weakness must be reported through the established communications channels. Any weaknesses that are identified by any member of staff that involve personnel, hardware, software, document, or physical security must be reported to the IT Security Manager. Where necessary weaknesses shall also be reported to clients where their data has been compromised.

'Security incident' means any incident (accidental, intentional or deliberate) relating to communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage the company.

The Incident response plan is tested once annually. Copies of this incident response plan is to be made available to all relevant staff members and steps taken to ensure that they understand it and what is expected of them.

Employees of the company will be expected to report to the CIM or SIRO for any security related issues.

The Company security incident response plan is as follows:

- Each department must report an incident to the CIM Response Team.
- That member of the team receiving the report will advise the Response Team of the incident.

- The Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of data and in mitigating the risks associated with the incident.
- The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties, as necessary.
- The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the CIM or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.

A department that reasonably believes it may have an account breach, or a breach of company information or of systems related to the environment in general, must inform the CMI and IT Incident Response Team. After being notified of a compromise, the CIM and IT Response Team, in consultation with the SIRO/DPO, will implement the Incident Response Plan to assist and augment departments' response plans. There are mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. Reports will be escalated to the Board of Directors detailing all security incidents along with recommendations for remedial action.

23. Information Security Incidents

Anyone suspecting that there has been, or is likely to be an information security incident, such as a breach of confidentiality, availability, integrity of information, or misuse of an information asset, should inform the ICT's Service Desk immediately. You may also contact any senior members of ICT or Company directly if you prefer to do so. The CIM or, if not available, the SIRO, has the authority to take whatever action is deemed necessary to protect the Company against breaches of security.

If the incident involves accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, you should report it immediately by completing a notification of data security breach from (accessible here).

In the event of a suspected or actual information security incident or an unacceptable network event, the CIM may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network.

Failure to report an information security incident or data breach may lead to disciplinary action being taken. If you are in any doubt regarding whether to report an incident, you should seek advice from ICT or the CIM.

In the event of any queries, questions, incidents or suspected breaches contact our:
Compliance & IT Manager (CIM) - Steve Maddocks
Tel: 01695 558420
Email: steve@sbskills.co.uk
or
Senior Information and Risk officer Owner and Senior Data Protection Officer
Neil Beaumont, Director
Email: neil@sbskills.co.uk

24. Security Education and Awareness

New users of IT facilities, staff, students and approved third parties, should be instructed on the Company policies and Codes of Practice relating to information security. They should also be given training on the procedures relating to the security requirements of the particular work they are to undertake and on the correct use of the Company's IT assets in general before access to IT services is granted. It is the responsibility of managers that their staff are suitably trained, and to maintain training records. They should be made aware in particular of this policy including the reporting procedures in section 7.
8.2 All new staff of the Company are expected to complete the Company's online security awareness training and a data protection e-learning course (these are currently included within SB Skills Solutions induction and on-going refresher training mandatory for all Company staff. Staff must also attend the IT security inductions when joining the Company and must be aware of the latest ICT security advice. This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable. Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

25. Review, Induction and Training

- All IG Framework Strategy Policies and Codes of Practice are reviewed and up-date annually or as a result of the application of new regulations or guidelines and are signed-off for publication, application and training at Board level.
- All Staff must evidence their reading and comprehension of all relevant Policies and CoPs as denoted in their Policy Review and Awareness training at induction and yearly thereafter.
- Completion of standard quarterly refresher/clarification training relating to these policies and CoPs is mandatory for all staff.
- Specific training for all staff and managers to ensure they are fully aware of their particular IG responsibilities and duties forms an integral part of the regular in-house monthly training schedule for staff at all levels.

- As well as Privacy Notice awareness training for students information governance and data protection policies are actively promoted and highlighted across the delivery spectrum and embedded in all service transactions.

Version History Version/Status
Comments

1.1/Approved	June 2018	Approved by Board of Directors
1.2/Approved	January 2019	Approved by Board of Directors
1.3/Approved	January 2020	Approved by Board of Directors
1.4/Approved	January 2021	Approved by Board of Directors

Next Review January 2022

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

____

Employee Name (printed)

____

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the Company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

____

Employee Signature