POLICY

IT Security

sustainable remuneration in a changing world

Contents

1. Policy Statement

"It shall be the responsibility of the IT Partner to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls."

This policy also sets out how 21st Century uses and protects any information that is obtained from its clients and/or prospective clients or suppliers. 21st Century is the Responsible Party as defined in the Protection of Personal Information Act, 2013 ("the POPI Act"). All information is processed and stored in compliance with the POPI Act and the Electronic Communications and Transactions Act ("the ECT Act)". 21st Century relies on the IT Partner to ensure adequate protection and confidentiality of information as defined in the POPI Act for 21st Century as the Responsible Party. It is incumbent on the IT Partner to keep 21st Century informed with immediate effect or as soon as it is within the knowledge of the IT Partner that any breach to the security of the information the IT Partner is protecting has occurred.

21st Century is committed to ensuring that the privacy of clients and/or prospective clients are protected through the I.T. Department. Should 21st Century ask clients and/or prospective clients or suppliers to provide certain information by which they can be identified, they can be assured that it will only be used in accordance with this privacy statement.

2. Collecting Information

21st Century may collect the following information:

- full name;
- identity number or passport number;
- contact information including email address;
- employment information such as name of employer and job title;
- demographic information such as race, gender, disability and other information required for the purposes of remunerate and terms and conditions of service;

- credit card or other information required to pay for the services, where required;
- remuneration data;
- other information relevant to reward, remuneration, terms and conditions of service and/or 21st Century consulting work;
- other information required for the purposes of supplier services.

3. Securing Personal Information

21st Century only secures and stores information on behalf of the corporate or individual clients and/or prospective clients or suppliers and this information will not be shared with any third parties without specific approval from clients and/or prospective clients or suppliers. 21st century will not sell, distribute or lease clients' and/or prospective clients' or suppliers' personal information to third parties unless specific approval has been obtained or are required by law to do so. Should clients and/or prospective clients or suppliers wish this information to be no longer stored they may advise 21st Century in writing and their information will immediately be permanently deleted.

In order to prevent unauthorised access or disclosure, 21st Century have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

Regarding information residing on a server or in a cloud 21st Century has secured such information by following best practices and stringent security guidelines for identity protection and ensuring it complies with all legislation and best practices for protection of personal information. To this end there are multiple layers of protection, including secure data transfer, encryption, network configuration and application and user level controls that are distributed across a scalable, secure infrastructure. Furthermore, access to the information is a considered decision, and is based on considerations of the need to work with specific data, and the need to access the data for project purposes. Typically, 21st Century staff and consultants will have access to the data as required. Upon joining 21st Century, IT support will be made aware of files or folders that the said individual should not have access to.

A complete audit trail is kept of all enquiries, amendments, additions or deletions to clients', and/or prospective clients' or suppliers' personal information. This audit log records the date and time of the activity as well as who accessed the information.

21st Century does not use cookies.

21st Century's website may contain links to other websites of interest. However, once clients and/or prospective clients or suppliers have used these links to leave our site, they should note that we do not have any control over that other website. Therefore, 21st Century cannot be responsible for the protection and privacy of any information which clients and/or prospective clients or suppliers provide whilst visiting such sites and such sites are not governed by this privacy statement. Clients and/or prospective clients or suppliers should exercise caution and look at the privacy statement applicable to the website in question.

Data Transfer Policy

Internal – Client data being transported within 21st Century (e.g. between members of a team) should take place making use of password protected files and only using email addresses from the 21st Century email domain (e.g. Gmail is not allowed). Only the minimum number of authorized employees should be included in the distribution list for any internal transfer of files. Only relevant employees should have access to the work folders required for them to perform their duties. This is administrated by our IT partner. Upon employment, 21st Century will complete a form detailing *per employee* the folders that the individual has no access to.

External – Clients may choose the manner in which they would like us to deliver their reports (it must be pre-agreed). Any electronic versions of reports must be password protected and sent to pre-authorised recipients on behalf of the client. The client may ask for a secure transfer of the files in which case a MS SharePoint site can be opened (specific to each client) and they can be given access to the information contained within the site (which provides 2 factor authentication).

Data Classification

- Restricted – Restricted data includes data that, if compromised or accessed without authorization, could lead to criminal charges and massive legal fines or cause irreparable damage to the company. Examples of restricted data might include proprietary information or research and data protected by state and federal regulations.
- Confidential - Access to confidential data requires specific authorisation and/or clearance. Types of confidential data might include ID numbers, cardholder data, M&A documents, and more. Usually, confidential data is protected by laws like the POPI Act.
- Internal - This type of data is strictly accessible to internal company personnel or internal employees who are granted access. This might include internal-only memos or other communications, business plans, etc.
- Public - This type of data is freely accessible to the public (i.e. all employees/company personnel). It can be freely used, reused, and redistributed without repercussions. An example might be first and last names, job descriptions, or press releases.

4. Summary of Main Security Policies

- Confidentiality of all data is to be maintained through discretionary and mandatory access controls.
- Internet and other external service access is restricted to authorised personnel only.
- Access to data on all laptop computers is to be secured through suitable protection, to provide confidentiality of data in the event of loss or theft of equipment.
- Only authorised and licensed software may be installed, and installation may only be performed by IT Partner staff.
- The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it will be removed from the workstation immediately.
- Data may only be transferred for the purposes determined in the Organisation’s data-protection policy.

- All removable media from external sources must be virus checked before they are used within the Organisation.
- All hard copies and encrypted removable media removed from the premises containing client information must be adequately protected. Any loss of information needs to be reported immediately for incident management and to mitigate risk.
- Passwords must consist of a mixture of at least 12 alphanumeric characters and must be changed every 30 days and must be unique.
- Workstation configurations may only be changed by IT Partner staff.
- The physical security of computer equipment will conform to recognised loss prevention guidelines.
- To prevent the loss of availability of I.T. resources measures must be taken to back up data, applications and the configurations of all workstations.
- A business continuity plan will be tested on a regular basis.

5. Cyber Supply Chain Risk Management

The PPRR risk management model is a popular global supply chain risk management strategy and is used by businesses around the world. The “PPRR” stands for:

- **Prevention -** Take precautionary measures for supply chain risk mitigation.
- **Preparedness -** Develop and implement a contingency plan in case of an emergency.
- **Response -** Execute on our contingency plan in order to reduce the impact of the disruptive event.
- **Recovery -** Resume operations and get things running at normal capacity as quickly as possible.

Manage environmental risk in the supply chain and ensure supply chain resilience by:

- **Multisource –** multiple sources mean multiple ways around a problem. Categorize suppliers not just by what we are spending, but also by potential impact if there’s a disruption.

- **Nearshore –** look to find suppliers and distributors closer to our center of operation and/or the end point of our supply chain to reduce cycle times for product development and delivery.
- **Stress test often –** mapping our supply chain network is just the first step. Comprehensive, and reoccurring, stress tests are the best way to check for vulnerabilities, some of which may lie hidden deep within the supply chain.
- **Invest in product and plant harmonisation –** the use of identical technology for different components allows greater flexibility in case of a disruption.

6. Virus Protection

- The IT Partner will have available up to date virus scanning software for the scanning and removal of suspected viruses.
- Corporate file-servers will be protected with virus scanning software.
- Workstations will be protected by virus scanning software.
- All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.
- No removable media that is brought in from outside the Organisation is to be used until it has been scanned.
- All systems will be built from original, clean master copies whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.
- All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.
- All demonstrations by vendors will be run on their machines and not the Organisation's.
- Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.

- New commercial software will be scanned before it is installed as it occasionally contains viruses.
- All removable media brought in to the Organisation by external consultants or IT Partner field engineers or support personnel will be scanned by the IT Department before they are used on site.
- To enable data to be recovered in the event of a virus outbreak regular backups will be taken by the I.T. Department.
- Management strongly endorse the Organisation's anti-virus policies and will make the necessary resources available to implement them.
- Users will be kept informed of current procedures and policies.
- Users will be notified of virus incidents.
- Employees will be accountable for any breaches of the Organisation's anti-virus policies.
- Anti-virus policies and procedures will be reviewed regularly.
- In the event of a possible virus infection the user must inform the IT Partner immediately. The IT Partner will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

7. Physical Security of Computer Equipment and Office Building

Physical Security of computer equipment will comply with the guidelines as detailed below.

Definitions

Area

Two or more adjacent linked rooms which, for security purposes, cannot be adequately segregated in physical terms.

Computer Suite

Mainframe, minicomputer, fileserver plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the mainframe, contained within a purpose built computer suite.

Computer Equipment

All computer equipment not contained within the ***computer suite*** which will include PC's, monitors, printers, disk drives, modems and associated and peripheral equipment.

High Risk Situation(s)

This refers to any room or ***area*** which is accessible

- at ground floor level
- at first floor level

Approved

Approved security system.

Personal Computers (PCs)

Individual computer units with their own internal processing and storage capabilities.

Intruder Alarm

An intruder alarm incorporating the following features should be installed. Installation, maintenance and monitoring by an ***approved*** company.

Protection of Signal Transmission

Unless telephone wires directly enter the protected premises underground, signalling to the ***Alarm Receiving Centre*** should be by direct line.

Location of Intruder Alarms

Detection devices should be located within the room or ***area*** and elsewhere in the premises to ensure that unauthorised access to the room or ***area*** is not possible without detection. This

should include an assessment as to whether access is possible via external elevations, doors, windows and roof lights.

Walktest

A walk test of movement detectors should be undertaken on a regular basis in order to ensure that all PC's are located within the alarm-protected area. This is necessary due to the possible ongoing changes in the position of furniture, screens and partitions, which may seriously impede the field of cover provided by existing detection devices.

For any PC which is not directly covered by an intruder alarm, the processing unit should have a ***lockdown device***.

Check Detectors

Locking personnel should ensure, as part of their normal duties at locking up time, that internal space detectors have not been individually obscured or had their field of vision restricted.

Alarm Zoning

The ability to zone the intruder alarm from the main control panel should be provided to enable authorised usage of other areas of the building outside normal hours, whilst retaining alarm detection within the room or ***area***.

Physical security

- 21st Century enlists the services of a professional security company who provides armed response services and alarm monitoring.
- The premises is secured by a remote security gate with an intercom and electric fencing.
- The server room is a secured vault with a vault locking door.
- 21st Century has a staff member who lives in accommodation on site.

8. Computer Suite

- The computer suite should be housed in a purpose built room.
- Partitions separating the room or ***area*** from adjoining rooms and corridors should be a minimum of 150mm solid non lightweight blockwork or brickwork devoid of glazing or other openings except for protected doors as defined below.
- The computer suite should contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure.
- No water, rain water or drainage pipes should run within or above the computer suite to reduce the risk of flooding.
- Power points should be raised from the floor to allow the smooth shutdown of computer systems in case of flooding.
- Solar power will be provided to the computer suite to help protect the computer systems in the case of a mains power failure.
- Access to the computer suite is restricted to IT Department staff.

9. Access Control

- Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- Where possible no one person will have full rights to any system. The IT Partner will control network/server passwords and system passwords will be assigned by the system administrator in the end-user department.
- The system administrator will be responsible for maintaining the data integrity of the end-user department's data and for determining end-user access rights.
- Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.
- Usernames and passwords must not be shared by users.

- Usernames and passwords should not be written down.
- All users will have an alphanumeric password of at least 12 characters.
- Passwords will expire every 30 days and must be unique.
- Intruder detection will be implemented where possible. The user account will be locked after 3 incorrect attempts.
- The IT Partner will be notified of all employees leaving the Organisation's employment. The IT Partner will then remove the employees' rights to all systems. Attached as Appendix E is the sign-out form completed on exit of an employee or consultant.
- Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example in cloud storage
- Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.
- File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Filescan rights to directories, files will be flagged as read only to prevent accidental deletion.

Clear Desk and Clear Screen

- All employees must log off (or place in sleep mode) or shutdown their computer when they are not working with it.
- All computers must be setup to enter sleep mode (and require the user to log in again) within 2 minutes of the computer not being used.
- All desks must be left clean and neat without any confidential information being present on the desk (all physical information of this sort must be locked/filed away).
- The clean desk policy is monitored continually within each team.
- Laptops and other portable computer devices may not be left unsecured and unattended at a desk
- Any printouts made by an employee must be immediately collected from the printer.

10. Business Continuity Plan

The following procedures shall be maintained in conjunction with the IT Partner (Current service provider):

- Daily backup of the entire server to onsite NAS device (Retention 2 weeks).
- Daily backup of the entire server to private cloud (Retention 2 weeks)
- Ongoing monthly back up, January through to December (retention 12 months); this is held offsite
- E-Mail confirmation of back up procedures to be forwarded automatically to the appropriate 21st Century and IT Partner personnel as processes are completed.
- IT Partner to provide “stress test” hardware for the purpose of disaster recovery tests on a three monthly cycle, being January, April, July and October.
- All laptops are connected to a centralised share folder, thereby ensuring central access to all 21st Century work and ensuring backup of data. All 21st Century work is housed via sharepoint, a secure place to store, organize, share, and access information from any device.

11. LAN Security

Hubs and Switches

LAN equipment, hubs, bridges, repeaters, routers and switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to IT Partner staff only.

Workstations

- Users must logout of their workstations when they leave their workstation for any length of time. Alternatively, Windows workstations may be locked.

- The IT partner sets all unattended workstations to enter auto lock mode after 1 hour.
- All unused workstations must be switched off outside working hours.

Wiring

- All network wiring will be fully documented.

Monitoring Software

- The use of LAN analyser and packet sniffing software is restricted to the I.T. Department.
- LAN analysers and packet sniffers will be securely locked up when not in use.
- Intrusion detection systems will implement to detect unauthorised access to the network.

Servers

- All servers will be kept securely under lock and key.
- Access to the system console and server disk/tape drives will be restricted to authorised IT Partner staff only.

Electrical Security

- In the event of a mains power failure, the solar power will provide sufficient power to keep the network and servers running until the generator takes over.
- Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.
- All UPS's will be tested periodically.

Server Specific Security

This section applies to Windows servers.

- The operating system will be kept up to date and patched on a regular basis.
- Servers will be checked daily for viruses.
- Servers will be locked in a secure room.
- Where appropriate the server console feature will be activated.
- Remote management passwords will be different to the Admin/Administrator/root password.
- Users possessing Admin/Administrator/root rights will be limited to trained members of the IT Partner staff only.
- Use of the Admin/Administrator/root accounts will be kept to a minimum.
- Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
- Users' access to data and applications will be limited by the access control features.
- Intruder detection and lockout will be enabled.
- The system auditing facilities will be enabled.
- Users must logout or lock their workstations when they leave their workstation for any length of time.
- All unused workstations must be switched off outside working hours.
- All accounts will be assigned a password of a minimum of 12 characters.
- Users will change their passwords every 30 days.
- Unique passwords will be used.
- The number of grace logins will be limited to 3.
- The number of concurrent connections will be limited to 2.

Wide Area Network Security

- Wireless LAN's will make use of the most secure encryption and authentication facilities available.
- Users will not install their own wireless equipment under any circumstances.
- All bridges, routers and gateways will be kept locked up in secure areas.
- Unnecessary protocols will be removed from routers.
- The preferred method of connection to outside Organisations is by a secure VPN connection, using IPSEC or pptp
- All connections made to the Organisation's network by outside organisations will be logged.

TCP/IP and Internet Security

- Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
- Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.
- Network equipment will be configured to close inactive sessions.
- All incoming e-mail will be scanned by the Organisation's e-mail content scanner via Office 365 basic.

Patch Management Process

- Identification of issue that requires patching
- Discussion between those requiring the patch and those that will be creating and deploying the patch.
- A backup / record of both the 'before' and 'after' versions of the system being patched must be retained in case of needing to revery back to a previous version.

12. Glossary

Access Control

The process of limiting access to the resources of a system only to authorised programs, processes, or other systems.

Audit Trail

A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticate

To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authorisation

The granting of access rights to a user, program, or process.

Discretionary Access Control

A means of restricting access to objects based upon the identity and need to know of the user, process, and/or groups to which they belong.

File Security

The means by which access to computer files is limited to authorised users only.

Firewall

A device and/or software that prevents unauthorised and improper transit of access and information from one network to another.

Ftp

File transfer protocol. Protocol that allows files to be transferred using TCP/IP.

Hub

Network device for repeating network packets of information around the network.

Identification

The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Internet

Worldwide information service, consisting of computers around the globe linked together by telephone cables.

LAN Analyzer

Device for monitoring and analysing network traffic. Typically used to monitor network traffic levels. Sophisticated analysers can decode network packets to see what information has been sent.

Laptop

Small portable computer.

Mandatory Access Control

A means of restricting access to objects based upon the sensitivity of the information contained in the objects and the formal authorisation of subjects to access information of such sensitivity.

Modem

Device which allows a computer to send data down the telephone network.

Password

A protected, private character string used to authenticate an identity.

Shareware

Software for which there is no charge, but a registration fee is payable if the user decides to use the software. Often downloaded from the Internet or available from PC magazines. Normally not that very well written and often adversely effects other software.

Telnet

Protocol that allows a device to login in to a Windows host using a terminal session.

UPS

Uninteruptable power supply. Device containing batteries that protects electrical equipment from surges in the mains power and acts as a temporary source of power in the event of a mains failure.

Username

A unique symbol or character string that is used by a system to identify a specific user.

Virus

Computer software that replicates itself and often corrupts computer programs and data.

13. Closing

The information contained in this document illustrates 21st Century's commitment to the protection of its client as well as its commitment to complying with the POPI Act as set out by the Information Regulator.

14. Appendix A

Electronic Mail Acceptable Use Policy

User Responsibilities

These guidelines are intended to help you make the best use of the electronic mail facilities at your disposal. You should understand the following.

The Organisation provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies and partner organisations.

When using the Organisation's electronic mail facilities you should comply with the following guidelines.

DO:

- Do check your electronic mail daily to see if you have any messages.
- Do include a meaningful subject line in your message.
- Do check the address line before sending a message and check you are sending it to the right person.
- Do delete or archive electronic mail messages when they are no longer required.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do take care not to express views, which could be regarded as defamatory or libellous.

DO NOT:

- Do not print electronic mail messages unless absolutely necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.

- Do not use excessive electronic mail for personal reasons.
- Do not send excessively large electronic mail messages or attachments.
- Do not send unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to several people.
- Do not participate in chain or pyramid messages or similar schemes.
- Do not represent yourself as another person.
- Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libellous.

Please note the following:

- All electronic mail activity is monitored and logged.
- All electronic mail coming into or leaving the Organisation is scanned for viruses.
- All the content of electronic mail is scanned for offensive material.
- If you are in any doubt about an issue affecting the use of electronic mail you should consult the I.T. Department.
- Any breach of the Organisation's Electronic Mail Acceptable Use Policy may lead to disciplinary action.

15. Appendix B

Internet Acceptable Use Policy

User Responsibilities

These guidelines are intended to help you make the best use of the Internet resources at your disposal. You should understand the following.

1. The Organisation provides Internet access to staff to assist them in carrying out their duties for the Company. It is envisaged that it will be used to look up details about suppliers, products, to access government information and other statutory information. It should be used for personal reasons in a responsible manner.

2. You may only access the Internet by using the Organisation's content scanning software, firewall and router.
   When using the Organisation's Internet access facilities you should comply with the following guidelines:

DO:

- Do check that any information you access on the Internet is accurate, complete and current.
- Do check the validity of the information found.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do inform the IT Partner immediately of any unusual occurrence.

DO NOT:

- Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- Do not download content from Internet sites unless it is work related.
- Do not download software from the Internet and install it upon the Organisation's computer equipment.

- Do not use the Organisation's computers to make unauthorised entry into any other computer or network.
- Do not disrupt or interfere with other computers or network users, services, or equipment.
- Do not represent yourself as another person.
- Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

Please note the following:

- All activity on the Internet is monitored and logged.
- All material viewed is scanned for viruses.
- All the content viewed is scanned for offensive material.
- If you are in any doubt about an issue affecting Internet Access you should consult the I.T. Department.
- Any breach of the Organisation's Internet Acceptable Use Policy may lead to disciplinary action.

16. Appendix C

Remote Access Security Policy

Wireless Access

Where the network is accessed remotely via wireless, appropriate wireless security standards will be used.

- Wired Equivalency Protocol (WPA-PSK) will be used as standard on Wi-Fi connections.
- A WPA-PSKencryption key will be used.
- The network will be configured not to advertise its presence.

- The power of access points will be turned down to a minimum that still allows the access point to function.
- Due to the possibility of cracking Wireless Encryption Protocol using sniffing software such as AirSnort all wireless access points will be outside the firewall.
- Wi-Fi Protected Access (WPA) will be used where it is available.

Secure Access via VPN

Access from remote users to the corporate network will be via secure IPSEC or PPTP VPN connections only. This is necessary to secure the connection from the remote device to the corporate network.

Prevention of Data Loss

- All laptops and PDA's that are taken off site will have the following security configured, to prevent data loss in the event of theft.
- The hardware password will be enabled if available.
- All corporate data on the laptop or PDA will be encrypted using appropriate encryption software.
- Sensitive documents will be accessed remotely and not downloaded to the laptop or PDA.

Remote Device Protection

- To prevent remote PC's, laptops, PDA's etc from compromising the corporate network, security software will be installed on the devices.
- Firewall software will be installed on the devices to prevent them from being compromised by trojans and back door software.
- Anti-virus software configured to automatically download the latest virus signatures will be installed and utilised.

Blue Tooth

To prevent Bluetooth enabled devices from being attacked and compromised the Bluetooth connections on mobile phones, PDA's and laptops will be disabled where appropriate. This is to prevent bluejacking, SNARF and backdoor attacks.

Standard Devices & Configurations

Devices that are used to access the network remotely, must meet the minimum standard for supported web browsers and operating systems, that is current at the time of access.

17. Appendix D

Choosing a Secure Password

User Responsibilities

In order to make it harder for people to guess your passwords please keep in mind the following advice:

- Don't use dictionary words - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.
- The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first thing potential crackers will try when guessing your passwords.
- Instead try to pick acronyms, mnemonics, random letters, etc., or insert non-alphabetic characters in the middle of the word, replace letters with numbers ('o' to zero, I to 1, E to 3), etc.
- Use a mIxTuRe of UPPER and lower case on case sensitive systems
- You must include a number (0-9) somewhere in the password. Try to fit this in somewhere inside whatever letters you choose, instead of at the end or beginning of the password.
- If possible include a symbol (£$%&^*+=) somewhere in the password.

- When changing passwords, change more than just the number: perhaps move its position within the password, add or subtract letters, change capitalisation, etc.
- However, choose something you can remember. This is very important; it is no good having a password like “h498cj3t34” if you have it written on a Post-It Note stuck to your monitor! If you must have a reminder or hint, use something cryptic that only you can understand.
- Never tell anyone else your password or allow them to log in as you. Avoid telling anyone your password on the telephone, hackers often ring up pretending to be from the Information Technology Department and ask for your password. If it is necessary to provide your password to someone else to allow a fault to be fixed, ensure that they are genuine members of Information Technology Department first.
- Try to avoid letting other people watch you key your password in. Choose something that is not easy to guess from watching, like “qwerty12345”.

18. Appendix E

Sign-out form for exiting employee

Upon resignation of an employee, the IT partner will be advised, with the following information confirmed:

- Confirmation of last date of backup to sharepoint
- date of last day in the office
- Backup and removal of data from personal machine, if applicable
- Removal of participant from mail distribution lists
- Forwarding of email to relevant manager
- Backup of email content as applicable
- Removal of participant from whatsapp group
- Removal of access to VPN and server

19. Version History

Version	Date	Description	Approved By
1.0	November 2021	Initial Policy Drafted	Bryden Morton
1.1	September 2022	Policy updated	Morag Phillips