INFORMATION SECURITY POLICY

DOCUMENT VERSION CONTROL – GOVERNANCE SCHEME

Date	Author	Version	Status	Reason for Change
Dec 2016	SEStran	1.0	Policy created	Implementation
Oct 2017	SEStran	1.1	Adoption of version control	Implementation
August 2018	SEStran	1.2	Adapted for Cyber Essentials Compliance	Implementation

INFORMATION SECURITY POLICY

1. Introduction

The objective of this policy is to ensure that SEStran and all its assets are adequately protected against threats to confidentiality, integrity and availability.

SEStran relies on information to fulfil its outcomes, goals and obligations. Information and the systems we hold and use represent an extremely valuable asset both to SEStran and potentially to others. The increasing reliance on information technology for the delivery of the services provided by SEStran make it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.

Threats to Information Security are becoming more widespread, ambitious and increasingly sophisticated. The consequences of the loss and misuse of confidential and sensitive information can not only be significant to the organisation but can be devastating to individuals. It is essential, therefore, that all information processing systems within SEStran, in whatever format, are protected to an adequate and effective level from disruption or loss of service or compromise whether through accidental or malicious damage.

It is necessary to have an Information Security Policy ('the Policy') to provide the guidelines and framework for ensuring that the confidentiality, security and integrity of information held by SEStran, its services and officers is maintained.
This policy should serve as a pillar and guideline for the development of the associated security policies, procedures and standards.

2. Scope

This policy applies to all employees of SEStran, contractors, visitors and anyone not employed by the organisation but engaged to work with or who have access to SEStran information, e.g. contractors or consultants who work through SEStran.

This policy applies to all locations from which SEStran systems are accessed (including home use). Where there are links to enable other organisations to have access to SEStran information, they must confirm the security policies they operate meet our security requirements or the risk is understood and mitigated. (With the exception of third party customers utilising SEStran systems.)

For the purpose of this policy, “Devices” shall mean all computers, laptops, telephone, smart phones, tablets and potable equipment.

3. Review and Audit

The SEStran Partnership Director is responsible for regular review of the policy in the light of changing circumstances. The review will occur annually or when there are significant changes. The Partnership Director has a responsibility to ensure that the policy is appropriate for the protection of SEStran's interests.

4. Content

Information is and should be considered as one of our most valuable assets. These assets should not be given away, stolen, modified without authorisation, or lost without trace or hope of recovery. Protecting our organisation from the threats against our assets is the responsibility of everybody.

Information can exist in various forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

We will define information security as the preservation of the following:

- Availability: Ensuring that quality information is available when needed.
- Confidentiality: Protecting business information from unauthorised disclosure.
- Integrity: Ensuring that business information can be relied upon by being protected from unauthorised alteration, faulty processing, destruction or loss.

Information security is achieved by managing and implementing a suitable set of controls. These controls may be implemented in the form of policies, procedures, organisational structure, and software or hardware functions. They ensure that every specific security objective SEStran defines as necessary is met, and ensure that the levels of confidentiality, integrity and availability achieved are acceptable under all circumstances.

The purpose of the Policy is to protect SEStran assets from all threats, whether internal or external, deliberate or accidental.

SEStran will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Access to information and other assets will only be given to those individuals whose duties require it and who have the necessary authority and security clearance
- Regulatory and legislative requirements will be met
- Information Security Training will be provided as part of Employee Induction
- All breaches of Information Security, actual or suspected, will be reported and investigated
- Standards will be produced to support the policy
- Business requirements for the availability of information and information systems will be met
- The policy and related procedures will be monitored and reviewed to ensure that they remain relevant and effective.
- All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff
- It is the responsibility of each employee to adhere to the Information Security Policy

5. Legal Requirements

Some aspects of information security are governed by legislation; the most notable U.K. Acts are:

- General Data Protection Regulation (2018)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Human Rights Act (2000)
- Equality Act (2010) (2012)
- Contracts Legislation
- Freedom of Information Act (2000)
- Local Government (Scotland) Act

6. Roles & Responsibilities

The objective of defining roles and responsibilities is to ensure that SEStran staff are aware of security risks and their responsibilities to minimise the threats.

SEStran's policy is to accept all reasonable obligations in respect of information security and to protect its information resources by implementing best practices that achieve an effective balance between cost and risk.

The Partnership Director is accountable for Information Security within SEStran.

Line managers, permanent and contract staff are all responsible for the day to day implementation of the Security policy.

7. Data Owner

Owners of data and information are expected to establish appropriate access controls for their data. Access to data should be limited to the appropriate set of people. Access is granted to employees when it is required for them to perform their jobs based on appropriate authorisation as defined by applicable policies and procedures. Access to certain data may be more restricted for legal and regulatory purposes.

Key responsibilities include:

- Data subject enquiry procedures as required by General Data Protection Regulation (2018).
- Preparing details of who can access what information, how and when, according to the particular classification of the information. Also refer to SEStran Publication Scheme http://www.sestran.gov.uk/uploads/12_05_16_sestran_guide_to_information_available_through_our_publication_scheme_v2.pdf
- Ensuring the system is maintained in an effective and controlled manner.

It is important to know the difference between a data controller and a data processor. A data controller is an organisation that determines the purposes for which, and the

way in which, personal data is processed. By contrast, a data processor is an organisation that processes personal data on behalf of the data controller

8. Management Duties

It is the responsibility of managers to ensure the following, with respect to their staff:

- All current and future staff should be instructed in their security responsibilities.
- Staff using IT systems/media must be trained in their appropriate use.
- Staff must not be able to gain unauthorised access to any of SEStran systems or data.
- Managers should determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.
- All staff should be aware of the confidentiality clauses in their contract of employment.
- Managers must ensure that HR and IT Services are advised immediately about staff changes affecting computer access (e.g. job function changes leaving department or organisation) so that access and privileges may be modified as appropriate and in accordance with Induction/Leaving processes.
- Managers must ensure that all contractors undertaking work for SEStran have signed any relevant confidentiality and/or non-disclosure agreements.

Managers should ensure that all staff have access to and have read this Information Security Policy.

9. Staff Duties

It is the responsibility of each member of staff to ensure that they:

- Perform no actions which may result in a breach of Information Security.
- Report any breach, or suspected breach of security to their manager or directly to the Partnership Director.
- Obtain, read, understand and agree to the responsibilities within this Information Security Policy and its associated documents.
- Do not expose or give access to data to someone who would not otherwise be granted access to it.

10. Acceptable Use

All use of computer systems, mobile devices and assets within SEStran will comply with the acceptable use terms below. For the purpose of this policy, “acceptable use” is defined as:

- Commercial activity for SEStran business
- Research, development and learning
- Personal educational development and learning
- Administration and management of SEStran business
- Development work and communication associated with the above
- Consultancy work contracted to SEStran
- Reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

Employees are reminded about Freedom of Information implications and right to privacy.
- Personal social media accounts are restricted due to risk from third party apps.

All use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

11. Inventory & Ownership

An inventory of all computer and equipment and software will be maintained. It is the responsibility of IT to detail each item of computer and telephone related equipment. This information will be maintained in a centralised asset inventory system held by SEStran and IT Service Desk. All employees will be asked to sign the register for mobile devices.

An up to date register of all proprietary software will be maintained to ensure that SEStran is aware of its assets and that licence conditions are followed. This register will be maintained by IT Service Desk. The purchase of any software must be approved by the Partnership Director and must conform to the SEStran Procurement Policy.

12. Software Usage

SEStran provides staff with the applications they require to perform their duties. It is therefore unlikely that any additional or external software will need to be imported or downloaded by individual users. In order to protect the integrity of our IT resources, the following rules must be followed at all times:

- All software within the company must have, and can only be used in accordance with, the appropriate licence agreement.
- Staff must not introduce or knowingly or recklessly transmit or distribute any bug, virus or rogue code of any format.
- Staff must not copy, remove or transfer software to any third party or non-SEStran equipment without written authorisation from the Partnership Director
- Staff must not modify software in any way, unless through authorised change control procedures.
- Staff must not corrupt, or attempt to corrupt, any data held within SEStran's computer systems.
- Staff must not use any software that has not been logged with and authorised by IT Service Desk.
- Staff must not load or install any purchased, donated or downloaded (including shareware or free software) onto any SEStran workstation without written authorisation from IT.

The use of pirated or illegal software or media (including movies and music) is strictly forbidden.

13. Hardware Usage

SEStran provides staff with the information technology systems and equipment required to perform their duties. It is therefore unlikely that any additional or external hardware will need to be installed or connected by individual users. In order to

protect the integrity of SEStran' IT resources, SEStran' employees and contractors must adhere to the following:

- Make no modifications to any computer equipment or install, or attempt to install, any additional piece of hardware into or connected to any device, without authorisation.
- Not connect or insert any form of storage medium to any device prior to obtaining recorded authorisation from IT technical support staff and attending IT to have the device virus checked on a stand-alone virus checker.
- Not tamper with or damage or do any act which may in any way affect the output or performance of any computer or telephone equipment.
- Not use SEStran computer equipment and systems (hardware or software) to send or knowingly receive any material which is offensive, abusive, indecent, obscene or menacing.
- Not connect to use, or allow to be used, any non-company equipment on the SEStran network or any other company device without authorisation. See laptop and remote access sections later in policy.
- Not physically relocate any company computer equipment within company offices. A request must be made to the Business Manager who will allow the move controlling any necessary connections and inventory changes and comply with any contractual arrangements with third parties.
- Not remove any equipment from any office or premises without specific or existing authorisation.
- Not use SEStran computer systems to operate a business, exploit business opportunities or solicit money for personal gain.
- Make every effort to ensure that all computer equipment is kept clean and fully functional, reporting any spillage, physical damage or event that may compromise the effective workings of any device.
- All unused or upgraded equipment including mobile telephones must be returned to the SEStran for re-use, sale or disposal.

All hardware is disposed of in a secure and environmentally friendly manner.

15. Telephony Usage

SEStran provides desk telephones for employees to aid their business function. Those using company desk phones must adhere to the following disciplines:

- Telephony services are provided for business use and personal calls, while permitted, should be kept to a minimum and be of a short duration.
- Telephony services should not be used for personal business reasons or personal gain.
- Telephony services should not be used to make abusive, threatening or menacing calls.
- A professional telephone manner should be used at all times.
- Take every reasonable precaution to protect equipment from damage, loss or theft. Such precautions should include not leaving portable devices or data unattended in an insecure place e.g. on the passenger seat of a car. Tracking function should be enabled on all mobile telephones.
- Immediately report any damage, loss or theft of equipment to the Business Manager

- Ensure that no unauthorised persons are allowed to use the device(s). Such use could allow access to company data.
- Ensure that all devices in this category are protected by a pin or password.
- Where a personal mobile device is used to access mail, this must be on the understanding that the device has a remote wipe, password protection and device encryption policy applied.
- Personal mobile phone usage on SEStran mobile telephones should be kept to a minimum during working hours and contained within call and data allowance.

16. E-Mail Usage

SEStran provides e-mail facilities to all staff to enable effective business communication. All email messages are virus scanned prior to being delivered to staff.

Users of the mail system should adhere to the following rules and guidelines:

16.1 Privacy

- Email is provided for the purpose of business correspondence and therefore employees should not expect privacy in anything they send, receive or store on SEStran' systems. Freedom of Information implications should also be considered.
- Access to mailboxes will be granted to management to read an employee's mail box where there is a legitimate reason to do so, for example, a person is absent and an important email is expected or to investigate suspected breaches of any organisational policy, rule or regulation.

16.2 Sensitive Information

- The sending of sensitive or copyrighted material, trade secrets or proprietary financial information without express written authority from the Partnership Director is strictly forbidden.

16.3 Legal

- The sending of any material that could be deemed abusive, threatening, defamatory, disparaging, libellous, criminal, pornographic or discriminatory is strictly forbidden. If unsure please refer to your manager for assistance. Please refer to SEStran Violence at Work Policy http://www.sestran.gov.uk/uploads/SEStran_Violence_at_Work_Policy.pdf
- Legal advice is, generally speaking, privileged. As such SEStran would not be obliged to disclose emails containing legal advice in any court or regulatory proceedings. This is a very important protection but one which can be lost if legal advice emails are disseminated widely. It is important therefore not to forward on any legal advice emails unless strictly necessary and not to do so to a wide group of people.
- Except where legal privilege applies, all emails, however confidential, may have to be produced in evidence in court proceedings so caution should be exercised when discussing matters of a confidential, controversial or disputed nature.

16.4 Personal Use

- Occasional personal use is accepted.. Overuse of systems for personal, non-business communication during working time or after hours is strictly forbidden.
- Sending personal emails directly to large distribution groups (mass mailings, chain letters etc.) is strictly forbidden.
- The use of the email system to pursue personal business interests is strictly forbidden.

17. WiFi

SEStran provides Wireless Internet communication facilities to enable effective business function and communication for all internal users with suitable devices and is not for personal use.

17.1 Guest Wi-Fi Access

The guest Wi-Fi facility is provided to allow visiting guests a particular level of service.

- Any Guest misuse of the service will result in an immediate exclusion.

SEStran accepts no liability for any harm to systems or data when making use of this facility.

18. Hacking, Cracking and Unauthorised Access

All users and contractors utilising company or client computer systems must strictly adhere to the following rules:

Any third party access must be authorised by the appropriate manager.

No user may use the company's Internet connection to deliberately disable or overload any computer or network (including the company's own network), or to circumvent any system intended to protect the privacy or security of another user.

Users must not intentionally seek information about, obtain copies of, or modify files, other data, or passwords belonging to other users, unless explicitly authorised to do so by those users.

Users may not attempt to circumvent user authentication or security of any host, network, or account, both internal and external. This includes, but is not limited to, accessing data not intended for the user, logging into a server or account the user is not expressly authorised to access, or probing the security of other networks.

The deliberate introduction of viruses, or malicious tampering with any computer system, internal or external, is expressly prohibited. Any such activity will result in disciplinary proceedings.

Users must not attempt to circumvent anti-piracy measures through code modification or the use of license keys obtained via key generator software ("Cracking").

19. External Devices (USB Sticks/Hard Dives/CD-R and DVD-R drives)

The use of external devices is only permitted upon application to the Business Manager. If approved, the Business Manager will issue an approved device for the staff member to use.

Any member of staff obtaining an external device must adhere to the following:

- Users are responsible for safe keeping of their work, USB Pen Drives, external USB hard drives, or external CD/DVD Rom drives.
- Loss of any SEStran external device must be reported immediately so that any potential risk can be appropriately assessed.
- Users must not attempt to alter or circumvent the device encryption in place on supplied external devices.

19.1 Prohibitions

- It is strictly prohibited to use any external device provided by SEStran for purposes other than that which intended.

19.2 Misuse

It is the responsibility of all staff that should you learn of any misuse or inappropriate use of software, hardware or mobile devices, you should immediately notify your line manager.

20. Data Management and Classification

Data access control decisions are appropriately distributed throughout the organisation and handled by Data Owners. Every piece of data and information in SEStran has an owner, the person or group responsible for determining how that data and/or information should be managed, classified and protected.

Owners of data and information are expected to establish appropriate access controls for their data. Access to data should be limited to the appropriate set of people. Typically, access is granted to employees on a need-to-know basis, when it is required for them to perform their jobs.

Nobody should attempt to circumvent access protection. When access is needed but not available, authorisation should be sought from the data owner.

If you are given access to data or information, you must maintain its established access policy. For example, you may neither expose nor give data to someone who would not otherwise be granted access to it.

SEStran classifies information as either public or confidential.

20.1 Public Information

Public information is that which has been intentionally and explicitly made available to the public. This does not include processed data from SEStran's services, even if the content was collected from public sources.

20.2 Confidential Information

Confidential information is any non-public information that is proprietary; licensed by; or entrusted to SEStran. It is everyone's responsibility to exercise due care and attention to ensure that confidential information stays confidential. Confidential information should not be shared with anyone unless proper authorisation has been granted.

Unless specified otherwise, all data within SEStran is considered Confidential and should be protected and treated accordingly, in line with SEStran Records Management Plan

21. Data Backup

While information can only be Public or Confidential within SEStran so data can be "live" or "recovery" or "archive".

21.1 Live Data

- SEStran provides all staff access to a network storage location with adequate storage for business needs.
- Data must be retained solely on network drives whenever it is practicably possible to do so in order to ensure routine backups capture users' live data – exceptions exist solely for onsite consultants with SEStran laptops but no regular access to SEStran networks.
- Data will be protected by a clearly defined and controlled back-up procedure which generates data for archiving and contingency recovery purposes.
- The backup copies will be clearly labelled and held in a secure area.
- The backup process will allow for the recovery of several generations of backup.
- Back-up data should be regularly tested to ensure it is sufficient and accurate.

21.2 Recovery Data

- Recovery procedures should be in place to recover to a useable point.
- Recovery data should be sufficient to provide an adequate level of service and recovery time
- Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.
- In order to ensure that corruption is not propagated to recovered data it should be thoroughly tested before being pushed to "Live".

21.3 Archive Data

- Archived data is information that is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes.
- Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location.

22. Equipment, Media and Data Disposal

It is a legal requirement of SEStran that should a computer ever have been used to process personal data, as defined by the Data Protection Act (1998), SEStran has to ensure the associated storage media should be disposed of only after reliable precautions to destroy the data have been taken.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive or confidential is being stored automatically on their hard disk.

Therefore, disposal of any IT equipment should only be arranged through the Business Manager who will arrange for storage media to be securely wiped, and supply a certificate of disposal.

23. Key Data Security Disciplines

23.1 Obligations

- SEStran holds confidential and personal information on a number of companies, Members, permanent and contract resources, past and current. Users must be aware of and adhere to the responsibilities imposed by the Data Protection Act (1998).
- SEStran holds detailed files and data relating to a number of organisations, contracts and agreements which must be treated with utmost confidentiality at all times.
- Users must report potential data security risks to their line manager or the Partnership Director.
- Users must always report any data loss or potential data loss to their line manager or the Partnership Director.
- Users must always ensure any data being sent out from the office is appropriately encrypted, consult the IT Service Desk if unsure.
- The obligation to keep information confidential continues after an employee's employment or contract with SEStran has ended, without limitation of time.
- In the case of printed materials always ensure they are marked with an appropriate statement of confidentiality.

23.2 Prohibitions

- Users must never issue any confidential or sensitive information to third parties unless they have obtained the necessary written authorisation to do so.
- Users must never use any company data for personal use or gain.

24. Physical Security

24.1 Offices and Premises

SEStran offices are located within Scottish Government premises and have a security entrance.

All staff and Consultants are issued with security identification badges and these should be worn at all times whilst on the premises. The transfer of badges, keys and other security devices is prohibited. Staff and Consultants leaving employment with SEStran must return all badges, keys and portable devices they have responsibility for.

To gain access, security passes must be presented and PIN number entered at the turnstile. Please contact the Business Manager is you forget your PIN.

Employee permitted hours of access are between 07:00 – 19:00 The security is designed to protect the fabric of the buildings as well as ensuring the physical security of all assets including organisational data.

A continuous dedicated reception/security service is provided for the main reception desk between 07:00 – 19:00. Access out-with these hours must be requested prior to visiting the offices.

Local network equipment is located in locked cabinets and where appropriate within secured areas and only staff or Consultants who have legitimate business and whose job require it should be allowed to enter areas where computer systems are located.

Confidential records are located in locked cabinets.

24.2 Visitors and Contractors

All visitors to SEStran premises should have official identification issued by Scottish Government reception/security personnel, be escorted at all times and their arrival and departure times recorded.

Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

There is a requirement for all managers to have a procedure in place for the secure control of contractors called upon to maintain and support IT equipment and software. The contractor may be on site or working remotely via a communications link.

24.3 Physical Security Disciplines

All information held on the networks including databases, file systems, documents and emails are the property of SEStran. This includes, but is not limited to, any such documents or information which you create and store on the company network.

24.4 Obligations

- Always ensure your external visitors report to reception.
- Be aware that external visitors may have access to your floor/office space.
- Keep a clear desk, securing any valuable equipment or data appropriately.
- Ensure confidential information is not left displayed on screens or desks while unattended.
- Think before you print in order to reduce the risk of unauthorised access to hard copies of sensitive data.
- Always ensure hardcopy is marked with a confidentiality disclaimer.
- Ensure any hard copy printouts containing confidential information are kept secure (and under lock and key where necessary) when non-SEStran employees such as cleaners and maintenance staff have access to the premises.
- Ensure any hard copy printouts containing confidential information are kept secure when accessing SEStran' network from a remote location.
- Use the shredder or contact the Scottish Government Facilities Services Helpdesk to destroy sensitive waste.

- Keep confidential records stored in locked filing cabinets..
- Any requests for additional lockable storage, where the personal lockable drawer unit and departmental lockable storage units are insufficient, should be made to your line manager.

24.5 Prohibitions

- Do not let unknown persons follow you into restricted areas of the office building.
- Staff must not attempt to gain access to areas which are normally restricted to them.
- Information must not be removed from SEStran premises without permission from the Partnership Director, and in line with the Data Protection Act (1998).

25. Network & Logical Security

25.1 Network Security

It is the responsibility of the Business Manger to ensure that access rights and control of traffic on all SEStran networks are correctly maintained. IT Service Desk will be responsible for implementing all required controls to access assets and data.

The Business Manager must maintain open communications with data and asset owners to ensure the IT Service Desk is informed of new users requiring access and those users who no longer need access either through changing job role or leaving the employment of SEStran.

It is the responsibility of IT to ensure that data communications to remote networks and IT facilities do not compromise the security of SEStran systems.

25.2 System Documentation

All systems should be adequately documented by IT Service Desk and should be kept up to date such that documentation matches the state of the system at all times.

System documentation, including manuals, should be physically secured when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

Distribution of system documentation should be formally authorised by the system manager.

System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.

25.3 Review

SEStran, in consultation with IT will conduct an annual review of its network infrastructure to ensure that it is utilising new technologies where appropriate and remains compliant with emerging best practices.

26. Logical Security Disciplines

26.1 Obligations

- Always ensure data being sent from the office is appropriately encrypted, consult the IT department if unsure.
- Always ensure appropriate disclaimers are in place where necessary.
- Ensure data is saved to the network drives and not to local hard disks so that appropriate backups are made and retained.
- Ensure you store personal electronic data to an appropriately secured and restricted area within SEStran systems.

- **26.2** Prohibitions
- Do not knowingly corrupt any data held within SEStran's computer systems.
- Do not load any data into any company system that has not been sourced internally or via customer uploads.
- Do not remove or upload to any third party site any company data from any company office or premises without specific authorisation.

26.3 Servers and networking

The installation and management of servers and networking equipment (such as routers, switches, firewalls, etc.) is the responsibility of IT.

All sites should be protected by appropriate security mechanisms such as Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), load balancers, etc. Security architectural decisions are a responsibility of the Partnership Director and IT.

There must always be a clearly defined owner for each device. The owner is typically the same person who requested the device and is normally the primary user. In the case of network connections, if IT is unable to determine the owner of a connection, they will disable it.

IT is also responsible for maintaining network, server, and application security. They should periodically audit the security of these devices and connections, validate that they are in compliance with the current secure configuration standards, and promptly address any concerns and recommendations raised as a result of these audits.

26.4 Patch Management

The IT Service Desk is responsible for Patch and Vulnerability management for the entire network including laptops, workstations, servers, networking devices, and supporting platforms.

All patches should be applied only after successful implementation in a testing environment, and the creation of a proper roll-back procedure.

However, critical patches should be applied not later than 48 hours of their release.

27. Passwords & Users

27.1 User Identification and Password Security

Your username and password identify you on SEStran systems. If you give someone else your password or through negligence allow them to obtain it then any subsequent actions performed by them, or any third parties to whom they

subsequently make it available, will be in your name. You will be held responsible for any activity or transactions carried out under your logon ID. With the exception of mailbox monitoring, during periods of annual leave and sickness absence.

It is therefore essential that all staff maintain good password security.

Poor password security can result in the compromise of SEStran entire corporate network. As such all employees (including temporary, contract and third party staff with access to information and/or systems) are responsible for taking the appropriate steps to secure their passwords.

Multiple staff access SEStran social media accounts using shared password credentials.

27.2 Password System Rules

As passwords are the primary preventative control mechanism for access to computer resources, where functionality permits, the system software will impose a limit of five invalid sign-in attempts before an account is locked out and require the use of complex passwords.

Complex passwords must contain three of the following four character groups and be at least seven characters in length:

- English uppercase characters (A through Z).
- English lower case characters (a through z).
- Numerals (0 through 9).
- Non-alphabetic characters (such as !, $, #, %).

Any password lockout will require helpdesk intervention.

Password protected screen locks are automatically initiated after 15 minutes of non-activity.

27.3 Password Disclosure

Should access be required to a particular system for which a password or security access has not already been granted, the user should contact their line manager to discuss whether they should be authorised to use this system and if a password or access can be issued.

SEStran employees and contractors must adhere to the following:

- Not solicit or attempt to solicit another user's password.
- Not log on to or use the system using another person's ID and password.
- Not disclose their password to any other users or third party. The only exception being a member of internal IT technical support for the sole reason of troubleshooting system issues. In this circumstance the password must be changed as soon as the issue has been resolved.

User access levels are subject to an annual review.

27.4 Password Protection

As well as avoiding direct password disclosure it is also the user's responsibility to prevent anyone else from acquiring their password by other means. Users should therefore:

- Never have a password that is easy to guess.
- Never write passwords down.
- Never allow anyone to observe you entering your password.
- Ensure that the 'Remember My Password' function of all applications is never selected and never enabled.

27.5 Password Changes

Passwords should be changed regularly. If at any time you suspect that someone else might know or have guessed your password, regardless of the length of time it has been in use, change it immediately.

All network passwords should be changed at least every 120 days; this will be set by network policy.

All system-level passwords (e.g. root, administrator etc.) must be changed at least every 30 days. Where functionality allows passwords will be auto-aged on this basis.

Any requests for a password reset should be directed to the IT Help Desk; the IT Help Desk may ask for proof of identity before performing the reset.

27.6 User Logon Disciplines

All users of SEStran systems must comply with the following general rules:

- Change passwords regularly (this will be enforced by the system where possible).
- Lock workstation when away from desk.
- Log off or reboot their workstation at the end of each day.

28. Remote Access

Remote access is defined as 'access to IT resources or data from a location external to the SEStran office.' It is the intention of SEStran to ensure that unauthorised use of or access to resources is kept to a minimum, and that risks including loss of confidential data, intellectual property, damage to internal systems and reputational risks are effectively mitigated.

Any remote access to SEStran systems requires authorisation from line manager, in line with the SEStran Home Working Policy.

http://www.sestran.gov.uk/uploads/SEStran_Home_Working_Policy_2016.pdf

Remote working users must:

- Immediately notify the IT help desk of breach of security of access credentials.
- Not carry out any sensitive or confidential work when in a place where 3rd parties could view information on the screen. This obligation applies even when working at home, if other individuals are or may be present.
- Give the same consideration to any remote connection as to their on-site connection.

- Not print out any confidential information unless absolutely necessary and dispose of confidential material using the appropriate method e'g shredder or sensitive waste uplift through the helpdesk. .
- Continue to adhere to all aspects of the Information Security Policy.

29. Malware & Threat Protection

Malware is one of the greatest threats to our IT systems. SEStran seeks to minimise the risks of malware through education, good practice and up to date anti-virus software on all computers.

Malware becomes easier to avoid if staff are aware of the risks with unlicensed software or bringing data/software from outside the organisation. Anti-virus measures reduce the risks of damage to the network.

IT centrally maintains and updates the currency of the virus definition files on servers and desktops, but users (especially peripatetic) are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from IT if any remedial action is necessary.

Computer viruses could cause major disruption to SEStran, its partners and its relationship with those partners, as well as considerable reputational damage. Through automated measures as well as staff and contractor vigilance, virus disruption to business operation should be kept to an absolute minimum

Users should report any viruses detected/suspected on their machines immediately to internal IT. No newly acquired disks from whatever source are to be loaded unless they have previously been virus checked by IT.

Users must be aware of the risk of viruses from emails and the Internet. If in doubt about any data received please contact IT Service Desk for anti-virus advice.

Malware Protection Principles

29.1 Obligations

- Particular attention must be paid when opening e-mail attachments, especially when containing macros that come from unknown, suspicious or untrustworthy addresses. If at all in doubt please do not open the attachment and contact the IT Service Desk.
- Any infection, data corruption or system damage (or threat thereof) must be reported immediately to the IT ServiceDesk.
- Never download or attempt to download files from unknown or suspicious source.
- Do not download or attempt to download any executable code from any web site. If this type of download is required please log a call with the IT Service Desk.
- Never open an email attachment unless you are expecting it.
- Never click on a link within an email asking for disclosure of personal information.
- Never download or attempt to install software to your computer.
- Never attempt to download files from file sharing sites such as RapidShare.

29.2 Prohibitions

- The removal or disabling, or any attempt to remove or disable, any antivirus software is strictly forbidden.
- Do not connect, or attempt to connect, any laptop, or any portable device to SEStran networks without prior authorisation from IT and a full virus check being performed.
- Do not connect, or attempt to connect any portable storage device for example USB sticks, diskettes, CDs/DVDs, digital cameras, personal mobile phones etc. from a source external to SEStran, to any SEStran networked device without prior authorisation from IT and a full virus check being performed.

30. Software

SEStran will only permit authorised software to be installed on its PCs or portable devices, which will be managed by the IT Service Desk. The company has a duty to ensure that all applications in use are covered by appropriate licensing details and associated Service Level Agreements and contracts (whether the software is free or not).

All software in use within SEStran must be centrally registered to ensure the company's licensing compliance and inventory details are accurate and that any testing environments during system upgrades are relevant and do not compromise the integrity of any testing due to missing applications.

30.1 Authorised software

SEStran will require the use of specific general purpose packages (e.g., word-processing, spreadsheets, and databases) to facilitate support and staff mobility:

- Non-approved packages should be phased out as soon as practicable unless there is a definable business use.
- Where SEStran recognises the need for specific specialised PC products, such products should be registered with IT Service Desk and be fully licensed.
- Software packages must comply with and not compromise SEStran standards.
- Computers owned by SEStran are only to be used for the work of SEStran.

30.2 Educational software

- Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by IT Service Desk.

30.3 Leisure software

Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained thereon.

- The installation of leisure software on to computing equipment, including mobile phones, owned by SEStran is not allowed.
- Installation of leisure software may result in disciplinary action under the Disciplinary Procedure.

30.4 Unauthorised software

Please note and adhere to the following rules governing unauthorised software usage:

- Any copying, installation or execution of third party software (including games, screen savers, mp3 files, etc.) from any external storage medium is strictly forbidden (this excludes IT technical staff for the purpose to fulfil their role only).
- Any downloading of any software or code of any format from the Internet or other on-line service to any of the company's computers, laptops, portable devices and mobile phones, is strictly forbidden (this excludes IT technical staff for the purpose to fulfil their role only).
- The use of pirated or illegal software or media (including movies and music) is strictly forbidden.

If you learn of any misuse or inappropriate use of software or related documentation, you should immediately notify your line manager or the IT Service Desk.

31. Exchange of Information

It is important for SEStran to function that information is able to flow efficiently between users and those on the outside who need that information without compromising its integrity and confidentiality

31.1 Sharing data/information with non-partner organisations

SEStran may receive requests for personal data. Organisations requesting such information may include but not to exclusion of others:

- The Police
- Insurance companies
- Solicitors
- Potential employers

SEStran will ensure that the provision of such information in fulfilling such requests is not abused and is in line with the SEStran Data Protection Policy.

32. Summary

It is the responsibility of every user to read, understand and adhere to this policy and to perform their respective duties in accordance with the policy.

Employees are expected to exercise good judgement regarding the legitimacy and reasonableness of their use of Information and IT resources at SEStran.

33. Review

The Partnership Director and Business Manager are responsible for reviewing this policy. This policy is to be reviewed under the following circumstances

- Annually
- In the event of any changes to legislation

Appendix A

Agreement Form

I have read and understand SEStran's Information Security Policy and agree to comply with these guidelines. I understand that any deliberate breach of these will be viewed seriously and may result in action being taken under SEStran's disciplinary procedures.

Please complete the details on this form and return to the **Business Manager, SEStran**

Name: _____

Job Title: _____

Signature: _____

Manager's Signature: _____

Date_____