Information Security Policy – S01

Document Control

Creator	Strata Compliance & Security Team
Source	Devon Information Security Partnership
Owner	Appointed SIROs
Subject	Information Security Policy
Protective Marking	OFFICIAL
Version	1.3
Version Date	January 2018
Last update	Robin Barlow – Supplier element

Target audience
Corporate

Contents

Authorisation Statement

This policy has been approved by the Councils and Strata as confirmed by each appointed SIRO as shown below and is a joint policy that applies to all parties.

Supporting sub documents will be independently approved and maintained under the stewardship of the SIROs of each organisation.

Exeter City Council

Signature:	Date:
Name:	Position:

East Devon District Council

Signature:	Date:
Name:	Position:

Teignbridge District Council

Signature:	Date:
Name:	Position:

Strata Service Solutions Ltd

Signature:	Date:
Name:	Position:

1 Introduction

The ICT services for the **"The Councils"** comprising Teignbridge District Council, Exeter City Council and East Devon District Council are provided by a wholly owned shared ICT service "Strata Service Solutions Ltd", referred to as **"Strata"**.

This common Information Security Policy applies to all the **"The Partners"** comprising of "The Councils" and "Strata".

1.1 Information is a major asset that the "The Partners" have a duty and responsibility to protect.

1.2 Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- speech

1.3 The purpose and objective of this Information Security Policy is to set out a framework for the protection of "The Partners" information assets:

- From all threats, whether internal or external, deliberate or accidental
- To ensure business continuity and minimise business damage
- To deliver its strategic and operational objectives
- To support data protection policies

1.4 The Information Security Policy is supported by a framework of supporting documents, some of which may be aimed at specific audiences:

- **Corporate** – Everyone
- **Councillors** – Elected members of each Council
- **Managers** – All Managers
- **Users** – All users of "The Councils" ICT, including employees, Councillors, Contractors and "Strata"
- **Strata** – Technical delivery staff employed by "Strata"
- **Third parties** –Organisations providing services to the Partners or working on behalf of the Partners;
- **Mobile information access** - Mobile Devices & Remote Working

1.5 The **"Information Security Policy Set"** refers to the combination of Information Security Policy and these supporting documents that may include:

- **Standards:** mandatory activities, actions, rules or regulations designed to provide decisions and limits for the policy components;
- **Procedures*:*** which define the details of how the policy, standards and guidelines will be implemented in an operating environment;
- **Baselines*:*** mandatory minimum acceptable values or types for security elements that must be met by the procedures and standards. These are often taken from industry standards;
- **Guidelines:** General statements designed to achieve the policy's objectives by providing a framework within which to implement controls not covered by procedures.

1.6 These are generally delivered by the specific “Partner” to allow for local naming and other requirements however the objective is for all “Partners” to align their policies/guidance to ensure consistency for users who may work across multiple organisations and also for the support of these users by Strata.

2 Scope

2.1 This policy applies to the staff, elected Councillors, temporary/contract staff, third parties and agents of “The Partners”, who have access to information systems and/or hold and process information for “The Partners’” purposes. It applies to all information assets of “The Partners”.

2.2 Information security principles apply to all information whatever the format or medium, including but not limited to, hard copy and soft copy such as manual files, handwritten notes, databases, CCTV images, speech recordings and magnetic media.

3 Risks of information security weaknesses

3.1 “The Partners” recognise the importance of information both in the provision of its services to the public and in order to facilitate its own operational needs and to allow for effective decision making at every level.

3.2 Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.

3.3 Poor education and training, misuse, and breach of security controls of information systems may result in data and information being put at risk, or it may be used to misrepresent the council and result in the ineffective use of council resources.

3.4 Information security incidents can give rise to embarrassment and loss of reputation, financial loss (fines), non-compliance with standards and legislation as well as possible judgements against “The Councils”.

4 Objectives and Aims

4.1 It is the policy of “The Partners” to ensure that information will be protected from a loss of:

- **Confidentiality:** information should only be accessible to authorised individuals.
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods.
- **Availability**: ensuring authorised users have access to relevant information when required.

4.2 “The Councils” will each appoint a security group that in this document will be referred to as the *Information Security Forum* (ISF) to review and make recommendations on security policy, policy standards, directives, procedures, incident management and security awareness education.

Each ISF will include a designated member of “Strata” and is the responsibility of each Partner SIRO to determine the composition that meets their organisation’s needs.

4.3 Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, Standards, Baselines and Procedures, which in turn will be incorporated into “The Partners’” operational procedures and contractual arrangements.

4.4 “The Councils” together with “Strata” will define an Information Security Management Process which will include the definition of information security incidents, data breaches and how they should be reported and managed.

4.5 Business continuity and disaster recovery plans will be produced, maintained and tested to provide continuation of service to ensure the security, confidentiality and availability of “The Partners” data.

4.6 “The Partners” will ensure the protection of their information assets are a priority.

5 Information security and handling awareness training

5.1 Information security awareness training is mandatory for existing employees and councillors and refresher training will be provided on an annual basis for all staff, including Strata staff.

5.2 “Strata” will assist “The Councils” with the creation and delivery of information security awareness training as part of its induction process for new employees and newly appointed councillors, and ongoing information security awareness training.

5.3 For clarity, “Strata” will ensure all Strata staff undergo security awareness that takes account of the additional privileges that Information Technology staff may have and include Data Protection awareness.

5.4 Specialised security training will be provided to staff who need to handle more sensitive data.

6 Responsibilities

6.1 “The Partners’” SIROs (Senior Information Risk Owners) are the owners of the “Information Security Policy Set”.

6.2 “The Partners’” SIROs have overall accountability for ensuring suitable management and individual responsibilities are in place to ensure physical assets, systems, processes and working practices comply with this “Information Security Policy Set”

6.3 The Council SIROs will each have the information management responsibilities of their organisation, and will mainly focus on the council’s specific data and conduct of their users. The Strata SIRO will predominantly focus on the technical data that supports the Strata infrastructure, and the Strata users.

6.4 “The Partners’” SIROs have responsibility to ensuring that suitable security incident reporting and management processes are embedded within their organisations.

6.5 It is the responsibility of all individuals who process and manage data on behalf of “The Partners”, to comply with information security procedures including data confidentiality, integrity and quality requirements.

6.6 Whilst Councillors are Data Controllers for their own data, they need to adhere to this policy when handling data originating from “The Councils”, for which they are not the Data Controllers. Councillors are also required to read and abide by the Councillors Addendum Sub Policy.

6.7 The appointed audit provider will work with “Strata” to review the adequacy of the controls that are implemented to protect the Council’s information and recommend improvements where deficiencies are found.

6.8 Contracts should be in place to ensure all third parties accessing “The Partners’” systems and information comply with the council’s Information Security Policy and its sub policies and components as appropriate.

6.9 Each “Partner” must have Data sharing agreements in place between “The Partners” to meet the needs of the Data protection legislation at the time.

6.10 Third parties will complete data sharing agreements where necessary, and comply with the relevant sub policies, such as the Third Party Use and Remote Access policy.

6.11 Failure to comply with the “Information Security Policy Set” may lead to disciplinary or other remedial action.

7 Communication

7.1 The “Information Security Policy Set” will be communicated to each employee, Councillor, contractor and relevant third parties accessing “The Partners’” information through a range of mechanisms and media, which may include intranets, websites, emailing, policy management programs and hardcopy (where appropriate).

7.2 Some Sub Policies, Standards, Baselines and Procedures will be selectively distributed dependent on the scope of each document.

7.3 Third parties and temporary staff/contractors should be made aware of “The Partners’” approach to Information Security. A Memorandum of Understanding (MOU) outlining the key requirements from this policy should be incorporated into supplier contracts and/or included in data sharing agreements if they are handling “The Partners’” data.

8 Compliance

8.1 The design, operation, use and management of information systems and the information processed within must take into consideration all statutory, regulatory and contractual security requirements.

8.2 “The Partners” are obliged to abide by all relevant UK and European Union legislation. The requirements to comply with this legislation shall be devolved to employees and agents of “The Partners”, who may be held personally accountable for any breaches of information security for which they may be held responsible.

8.3 In order to facilitate information security, “The Partners” shall comply with the legislation as listed in Appendix B and other applicable legislation as appropriate.

9 Information security policy set

9.1 Key policy areas

9.1.1 There is an expectation that the “Information Security Policy Set” for all partners will cover these key areas that are described in more detail in the following sub-sections:

Information Security Policy Set	Mandatory for all
Acceptable Use	**Y**
Mobile Devices & Remote Working	**N**

Information Protection	**Y**
Security Incident	**Y**
Third party use of IT and Remote Access	**N**
Councillors addendum	**N**
Corporate and IT providers	**N**

9.2 Acceptable Use

9.2.1 Covers the most common usage of “The Partners’” IT systems including: email; internet browsing; instant messaging; system access credentials (passwords) and general acceptable care and usage of the IT systems.

9.3 Mobile Devices & Remote Working

9.3.1 Supports the controlled storage and transfer of information by councillors, employees, temporary staff and agents (contractors, consultants and others working on behalf of “The Partners”) who use “The Partners” IT systems outside the office environment, or with equipment not physically connected to the IT network but able to access “The Partner” systems.

9.3 2 It will cover the approved methods and usage requirements for remotely accessing the internal council systems including expectations of up to date malware protection on personal devices.

9.4 Information Protection

9.4.1 The purpose and objective of this document is to specify the means of information handling and transfer within the “The Partners” through the appropriate marking of “The Councils” data and processes and procedures.

9.4.2 This should either reference or be the individual “Partners’” Data Protection policy and procedures.

9.4.3 For clarity, this will also include USB data storage devices including ‘memory sticks’ and portable ‘hard drives’.

9.5 Security Incident

9.5.1 This document must stipulate the processes that must be followed by each “Partner” in the event that an information security incident occurs when the confidentiality, integrity or availability of information is either confirmed, suspected or there was a narrow avoidance of this type of event.

9.5.2 With the “Partners” sharing the underlying IT systems there is a duty on each “Partner” to inform the other “Partners” of any incident that impacted or risked the others systems or data.

9.6 Third party use of IT and remote access

9.6.1 This will be maintained by Strata and details requirements for allowing entities, usually suppliers of IT services, managed access to the “Partners’” IT systems.

9.7 Councillors addendum

9.7.1 This will record any differences in the requirements for Councillors, for example that many are their own Data Controller for data protection.

9.8 Corporate and IT Providers

9.81 This details the expectations of the IT provision from Strata and external providers and in general covers technical details of the provision and specific policy expectations for providers.

9.82 This will also cover hosted system and the security requirements of the providers of these systems.

9.83 This also covers physical and environment requirement requirements for all Partners to ensure the Security, Integrity and Availability of the IT Systems and data.

9.84 The Strata SIRO is responsible for the maintenance of this policy in conjunctions with the other Partner SIROS

10 Monitoring

10.1 “The Partners” reserve the right to monitor all its Information Systems in order to ensure legislative, policy and legitimate business requirement compliance in accordance with the legislation in Appendix B, which would normally be to:

- Establish the existence of facts relevant to the business, client, supplier and related matters
- Ascertain or demonstrate standards which ought to be achieved by those using the facilities
- Check compliance with approved Council policies and procedures
- Prevent or detect crime
- Support the interests of national security, following the appropriate authorisation
- Investigate or detect unauthorised use of the Information Systems
- Ensuring effective operation of the information systems, including their security

10.2 To provide monitoring capabilities, technical logging of the systems usage will be captured and stored in accordance with the legislation in Appendix B. Where necessary, previously deleted emails may be restored to assist with an investigation.

10.3 “The Partners” do not examine the content entered through the information systems as a matter of course, however it may apply manual and/or automatic monitoring, filtering and rejection as appropriate when it is considered there may be unacceptable use or valid security threats. Examples of ‘content’ include emails, instant messages (Twitter, Skype, Facebook, iMessages, telephone SMS) and web page content.

10.4 The content will not be examined where it can be categorised as personal information, and any such information that is subsequently found to be personal will be treated in the strictest

confidence. To assist the examiner any content marked 'personal' (in the subject, folder/container name, filename) will not be examined unless there are convincing grounds on which to believe they are in fact business related.

10.5 Only authorised employees will undertake the examination of this content, and only as part of an agreed monitoring process or investigation. The authorisation process for each 'Partner' will be defined by the respective SIRO.

11 Breaches of the "Information Security Policy Set"

11.1 All breaches of "the Information Security Policy Set" must be reported through the agreed incident reporting mechanism. In the event that this breach may involve an identifiable individual, then this should be reported through the relevant Head of Service or SIRO, or for Councillors through the Monitoring officer or Chief Officer.

11.2 Where external service providers, agents or contractors cause a breach, this should be addressed through contractual arrangements.

11.3 The Strata Compliance and Security Manager will be responsible for investigating all security breaches that relate to security of the IT systems. The SIROs and council officers will be informed and consulted to ensure that any investigations are fit for purpose and do not compromise any local activities.

11.4 For all non-IT security breaches it will be the responsibility of the associated organisation to investigate, and where appropriate communicate the findings to "The Partners'" SIROs.

11.5 Where the public have access to "The Partners" IT systems, that access will be withdrawn if there is an actual or likely breach of information security, until adequate controls are in place.

12 Exception management and review

12.1 There may be times that elements of the "Information Security Policy Set" may not meet the business requirements. In these cases a formal process will need to be followed to consider the need and assess any impact to the information security objectives.

12.2 The "Information Security Policy Set" has been intentionally structured to be managed at different management levels within "The Partners".

Documents	Change process	Signoff process
Security Policy	Responsible: SIROs Reviewed every two years The policy elements included should require little change.	Council signoff as per each Council's requirements for major and minor amendments and Board signoff for Stata.
Sub Policies, Standards, Baselines, Procedures, Guidelines	Responsible: SIROs, with all changes notified to the Strata Compliance and Security Manager Reviewed annually unless exceptions/ changes are required.	SIROs supported by the ISFs

12.3 Where changes are required these will be considered by the relevant group or role holder in the 'Change process' column above.

12.4 For all changes that need some urgency, the initial change may be authorised by the Strata Compliance and Security Manager who will seek to limit the scope, duration and impact of the change and treat it as an exception. Exceptions will be reported to the SIROs.

12.5 The periodic review of the documents will review requested changes, exceptions and ensure that documents still meet the information security management needs of the “Partners”.

Appendix A: Glossary

Term	Description
Baselines	Establishes the minimum acceptable values and types of implementation methods for each security item. In general this should be based on external standards and best practice. A password minimum is an example.
Data	A specific fact or characteristic.
Devon Information Security Partnership	Representatives of the Local Authorities and other Government organisations in the County of Devon. This group initiates and supports good information security practice.
Guidelines	General statements designed to achieve the objectives of the policy by providing a framework within which to implement controls.
ICT/IT	Information Communications Technology / Information Technology.
ISO	International Standards Organisation.
Information	Data being used in context and usually for decision making.
ISF	An Information Security Forum consists of representatives from each “Partner” that monitors and support the implementation of this policy and recommends how the policy should apply to Council activities. The ISF also helps define changes to the policy.
Logging	Technical recording of usage, changes and status information, that supports monitoring.
Monitor	Technical and manual processes that allow for real time and retrospective analysis of the usage of the systems in question.
PSN	Public Services Network is a Government secure network which allows Councils to communicate and share data securely with each other, Central Government and its associated organisations. The PSN also facilitates access to secure systems owned by Government departments such as the DWP.
Procedures	Step by step instructions detailing how policy and standards will be implemented in an operating environment
SIRO	Senior Information Risk Owner is a board-level or similar individual who is responsible for Information Security within an organisation.
Standards	Mandatory activities, actions, rules or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective.

Appendix B: Legislation

Data Protection Act (1998)	Principle 7 of the Act requires that *"appropriate technical and organisation measures"* are implemented to protect data. This will be replaced by the Data Protection Bill
General Data Protection Regulation (GDPR)	Valid from May 2018 and widens the scope of personal data and significantly increases the penalties.
Data Protection Bill (2017)	This needs to be read alongside the General Data Protection Regulation as it both defines the UK approach on certain optional GDPR areas and also defines some areas not included in GDPR (mainly security services).
The Human Rights Act (2000)	Article 8 of the Act requires that the Trust maintains the *"right for respect for private life."*
The Employment Practices Data Protection Code	Part 3: Monitoring at Work *"Any adverse impact of monitoring on individuals must be justified by the benefits to the employer and others."*
Privacy and Electronic Communications Regulations 2003	Prevention of nuisance or unsolicited communication to other parties
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.	The council maintains the legal right to monitor and audit the use of Council email systems to ensure adherence to this policy.
Regulation of Investigatory Powers Act 2000	The council may intercept emails in order - to establish facts - to find out if a communication is for business or private purpose - for quality control or training - to comply with regulatory or self-regulatory procedures - for system maintenance - to detect unauthorised use - to prevent or detect crime - for national security purposes