districtnk

Title: Statement of Security of Information Assets	**Approved**: Draft Approved On 01/09/2016	**Effective from**: 01/09/2016	**Next review**: 20/09/2019
Version: 3	**Author**: Cliff Dean		**Last review**: 11/09/2018

Aim

To provide an annual statement of the security of information assets, protecting the data that we collect and store securely. Key roles within the council maintain the privacy of individuals and deliver Information Assurance (IA) Senior Information Risk Owner (SIRO), System Owner (SO), Chief Information Owner (CIO IT), Data Protection Officer (DPO) and the Information Asset Owner (IAO).

All colleagues understand that the information we hold is valuable. We are committed to preserving the confidentiality, integrity, and availability of our information assets:

- for sound decision-making;
- to deliver quality services to our citizens and customers;
- to comply with the law;
- to meet the expectations of our customers and citizens; and
- to protect our reputation as a professional and trustworthy organisation.

Problems with any information we hold can cause issues for our staff, business, customers, citizens, and third parties. Information security is everyone's responsibility.

Scope

The Council has a strong information assurance structure which ensures that access to data is controlled and only provided to those that need it for the required duration. System Owners and Information Asset Owners are senior individuals that manage the risk associated with the use of data.

Definitions

Information Asset Owners role is to understand what information is held for their own business area, how that information is used, who has access to it and why. As a result they are able to understand and address risks to the information, ensure that information is used appropriately, and provide input to the SIRO on the security and use of their information asset whether in paper or electronic format.

Principles

It is important that citizens are able to trust the council to act appropriately when obtaining and holding information and when using the authority's facilities. It is also important that information owned by other organisations which is made available to the Council under secondary disclosure agreements is treated appropriately.

Access Control and Asset Management

To control the access to information, stringent access controls are applied to any area or system where sensitive or protectively marked data is stored. Asset and configuration management controls are also in place and access to IT equipment and systems is strictly controlled.

Removable media, such as laptops have encryption added which has been approved by CESG. USB memory devices are disallowed as standard and access to secure devices is only provided through a request, record and approve process.

The IT Team takes particular care during the life cycle of an information asset. Members of IT are subject to a disclosure and baring service review. Controls are in place when the data is stored (e.g. secure server rooms), when data is in transit (e.g. use of encryption) and when disposal is required (following the guidance provided by CESG).

HR Security

All staff employed by the Council are required to undergo pre-employment checks.

After taking up duty, all new staff attend induction training that covers data security principles. Staff also have to complete the Data Protection and Information Assurance training package. The council keep statistics of all training completed.

Staff who use information processing facilities are subject to the conditions of the Corporate IT Access Policy.

Physical Security

To prevent unauthorised physical access, damage or interference to council premises and information, all council buildings are secured. Access to data storage areas is further secured with an additional alternative solution.

Incident Management

To ensure information security events and weaknesses associated with any council assets are captured, the council has a well-established incident management process and uses regular IT Health Checks to enhance security and monitoring. All reports are documented, followed up and reported to Senior Management.

Business Continuity

The Council has an excellent and robust approach following the national standard for business continuity. The management of IT assets to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters, the council have defined business continuity plans, procedures, roles and responsibilities.

Background Legislation

Data Protection Act 2018

Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it. Unauthorised disclosure of council or client personal information is prohibited and could constitute a breach of this Act.

Computer Misuse Act 1990

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is not allowed and would constitute an offence under this Act for which the penalties are imprisonment and/or a fine. This Act addresses the following offences:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

Copyright, Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.

Companies Act 1985

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

Freedom of Information Act 2000

This Act gives a general right of access to all types of data and information that has been recorded by the council.

The Council is also progressing its compliance activities associated with General Data Protection Regulation.

PCI DSS

Is the core PCI standard as it applies to any organization that stores, processes, and/or transmits cardholder data. This includes businesses, processors, acquirers, issuers and service providers. Literally every entity in the payment processing industry.