Bilsington Parish Council.

Information Security Incident Management Policy

1. Introduction

Bilsington Parish Council is responsible for the security and integrity of all data it holds. The Council must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the Council's assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security;

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
  - Loss of confidentiality of information
  - Compromise of integrity of information
  - Denial of service
  - Unauthorised access to systems
  - Misuse of systems or information
  - Theft and damage to systems
  - Virus attacks
  - Intrusion by humans
- Other incidents include;
  - Missing correspondence
  - Exposure of uncollected printouts
  - Misplaced or missing media
  - Inadvertently relaying passwords
  - Loss of mobile phones and portable devices.

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent incidents occurring.

More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

2. Purpose

The management of security incidents described in this policy require the Council to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide guidance

3. Scope

This policy applies to:

- Council employees, elected members, partner agencies, contractors, volunteers and vendors

- All Council personnel and systems (including software) dealing with the storing, retrieval and accessing of data.

4. Policy Statement

The Council has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing Council employees, elected members, partner agencies, contractors, volunteers and vendors of the importance of the identification, reporting and action required to address incidents, the Council can continue to be pro-active in addressing these incidents as and when they occur.

All Council employees, elected members, partner agencies, contractors, volunteers and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via the Council's Incident Reporting procedures.

The types of incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended

Users of Council computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Council employees, elected members, partner agencies, contractors, volunteers and vendors need to ensure that they lock their computers appropriately – this must be done despite the fact that Council computers are configured to automatically lock after 10 minutes of idle time.

Discovery of an unlocked computer which is unattended must be reported via the Council's Incident Reporting procedures.

Password disclosures

Unique ID's and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedure for authorisation.

Virus warnings/alerts

All computers across the Council have antivirus (including Anti-spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Council data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported as soon as possible.

Media loss

Use of portable media such as CD/DVD, USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any unauthorised user of a portable device (including portable media) who has misplaced or suspects damage, theft whether intentional or accidental must report it immediately through the Council's Incident Reporting procedures.

Data loss/ disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised recipient (such as the use of email to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Council's website and identified as inaccurate or inappropriate
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All Council employees, elected members, partner agencies, contractors, volunteers and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Council data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using the Council's Incident Reporting procedures.

Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank details etc. must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person identifiable information must be reported through the Council's Incident Reporting procedures.

Physical security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower/floor level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data.

Logical Security / Access Controls

Controlling, managing and restricting access to the Council's databases and applications is an essential part of Information Security. It is necessary to ensure that only authorised employees can gain access to information which is processed and maintained electronically.

Missing correspondence

Data or information which has been sent either electronically or physically which_cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no print output retrieved etc., must be reported through the Council's Incident Reporting procedures.

Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported vis the Council's Incident Reporting procedures.

<u>Loss or theft of IT/information</u>

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinets, etc., or which is known/or suspected to have been stolen needs to be reported immediately through the Council's Incident Reporting procedures.

5. Responsibilities

It is the responsibility for all Council employees, elected members, partner agencies, contractors, volunteers and vendors who undertake work for the Council, on or off the premises to be proactive in the reporting of security incidents. The Council's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Council data and information.

It is also a responsibility of all individuals and handlers of Council data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

6. Compliance with legal and contractual obligations.

The Data Protection Act (1998) requires that personal data be kept secure against unauthorised access or disclosure.

The Computer Misuse Act (1990) covers unauthorised access to computer systems.

7. Breaches of Policy

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Council assets, including IT equipment and information, or conduct which is in breach of the Council's security procedures and policies.

All Council employees, elected members, partner agencies, contracts, volunteers and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, volunteers, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee, infringements will be investigated under the disciplinary procedure and progressed as appropriate.

8. Incident Management

All parties dealing with security incidents shall undertake to:

- Analyse and establish the cause of the incident and take any necessary steps to prevent recurrence
- Report to all affected parties and maintain communication and confidentiality throughout investigation of the incident
- Identify problems caused as a result of the incident and to prevent or reduce further impact
- Contact 3rd parties to resolve errors/faults in software and to liaise with the relevant parties to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Council systems and services
- Ensure all systems logs and records are securely maintained and available to authorised personnel when required
- Ensure only authorised personnel have access to systems and data
- Ensure all documentation and notes are accurately maintained and recorded
- Ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness

Where appropriate, incidents will be presented to the full Council via the agenda and will be included on the Corrective and Preventative Action log.

All incidents logged shall have all the details of the incident recorded – including any action/resolution, links or connections to other known incidents, incidents which were initially resolved but have recurred will be reopened or a new incident referencing the previous one will be created.

During the course of incident investigations, hardware, logs and records may be analysed by the Council's internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential during the course of these investigations that confidentiality is maintained at all times.