ANGUS COUNCIL

INFORMATION TECHNOLOGY (IT) SECURITY POLICY

Version:	V01
Author(s):	Colin Milne, IT Security Consultant
Date of Approval:	October 2018
Approved by:	Information Governance Steering Group
Date issued:	October 2018
Next review date:	September 2019

Document Control Sheet

Author(s): Colin Milne, IT Security Consultant

Document Title: Angus Council Information Technology (IT) Security Policy

Review/Approval History

Date	Name	Position	Version Approved	Date Approved

Version	Date	Brief Summary of Changes	Author

Contents:

1. INFORMATION TECHNOLOGY (IT) SECURITY POLICY

The continuing availability of information systems is essential to the operation of Angus Council. For this reason information systems must be recognised as a major council asset and be protected accordingly. Protecting these information systems and the investment that surrounds them is the purpose of this Information Technology (IT) Security Policy.

Council information systems used to enter, process, store, generate, or disseminate information must be protected from misuse, unauthorised modification, damage, or disclosure by individuals internal or external to the organisation.

By selecting and implementing the appropriate controls identified risk can be reduced to an acceptable level. These controls are selected taking into account the need to preserve the confidentiality, integrity and availability of the information and systems. Non-monetary factors such as loss of reputation are also taken into account.

Operational procedures must be established to implement the corporate IT security requirements outlined in this Information Technology (IT) Security Policy, and appropriate mechanisms put in place to monitor and manage these procedures.

This Information Technology (IT) Security Policy is supplemented by an "Information Security User Guidelines" document.

2. SCOPE

The implementation of this policy will help to ensure the protection of the council's IT infrastructure, which is taken to include (but is not restricted to) –

- All physical data communications networks and components.
- All computer systems, accompanying operating system software and installed software applications.
- All corporate software applications.
- All storage and backup systems.
- All IT related system and software applications documentation.

3. RELATED DOCUMENTATION

Information Security Policy
Information Security User Guidelines
E-mail and Internet Usage Policy
Password Policy and Guidelines
Data Protection Act 2018
Computer Misuse Act 1990

4. SECURITY ORGANISATION

A management framework will be established to initiate and control the implementation of IT security within the organisation.

The relevant Strategic Director will serve as the designated officer responsible for developing, publishing maintaining and administering the Information Technology (IT) Security Policy.

Heads of Service are deemed to be owners of their service information assets. They may delegate their security responsibilities to individuals or service providers, nevertheless the owner remains ultimately responsible for the security of the asset and should be able to determine that any delegated responsibility has been discharged correctly.

Implementation of the Information Technology (IT) Security Policy will be independently reviewed to ensure that practices laid down within the policy are feasible and effective and are being adhered to.

5. SECURITY OF THIRD PARTY ACCESS

To maintain the security of council IT systems and information, access to council systems by (non-organisational) third parties will be rigorously controlled.

6. ASSETS CLASSIFICATION AND CONTROL

To ensure that information assets receive an appropriate level of protection, security classifications will be used to indicate the need and priority.

The Service Manager Digital Enablement and IT will maintain a computer based inventory register which will fully address the requirements of the council's Audit or Inventory Procedures. This register will include all major items of the council's IT infrastructure. Heads of Service will maintain an inventory of systems, software, applications and data owned by or licensed to their service.

The responsibility for classifying and declassifying departmental information assets will reside with the designated asset owners. The Service Manager Digital Enablement and IT will be responsible for classifying and declassifying corporate information assets.

7. PERSONNEL SECURITY

The Council's Leadership Team will take all appropriate measures to minimise the risks of human error, theft, fraud or misuse of the council's information assets and systems. In addition, steps will be taken to ensure that all users of the council's information systems are made aware of security risks and are equipped to adhere to, and support, the council's Information Technology (IT) Security Policy in the course of their normal duties.

8. USER TRAINING

The Council's Leadership Team will ensure relevant IT security training will be given to the users of the council's information systems.

9. RESPONDING TO INCIDENTS

All council staff have a responsibility to report suspected breaches of this Information Technology (IT) Security Policy to their own service management who will in turn ensure that any security incidents will be recorded by means of a formal logging and follow-up process.

Unless authorised by the Service Manager Digital Enablement and IT, staff will on no account attempt to replicate or simulate any suspected security breach or incident. Council staff suspected of being in breach of the council's Information Technology (IT) Security Policy will be subject to investigation under established formal disciplinary procedures.

10. PHYSICAL AND ENVIRONMENTAL SECURITY

Appropriate control mechanisms will be established to prevent unauthorised access, damage and interference to council information systems, including all physical information assets which support critical or sensitive activities.

11. REMOVAL OF PROPERTY

Removal of property or information belonging to the council is prohibited without prior authorisation by the asset owner.

Any piece of council IT equipment authorised for use outwith council premises, including but not restricted to laptop computers, phones and tablet devices, will be subject to the same guidelines for use as IT equipment within the workplace.

Whilst off-site or in transit, such equipment will be protected by the user from the risk of theft and will not be left unattended in public places.

12. COMPUTER AND NETWORK MANAGEMENT

To ensure the correct and secure operation of computer and network facilities responsibilities and procedures for the management and operation of all computers and networks will be established.

13. PROTECTION FROM MALICIOUS SOFTWARE

To safeguard the integrity of software and data no unlicensed or unauthorised software will be permitted on any of the council's IT systems.

Data files may only be downloaded from external sources in accordance with the council's "E-Mail and Internet Usage Policy".

Council employees must read and comply with the council's "E-mail and Internet Usage Policy".

Pro-active measures will be taken to safeguard the integrity of software and data by detecting and counteracting the effects of 'malicious' software such as computer viruses. This will include the provision of virus detection (endpoint protection) software on the council's computer systems.

Pro-active measures will be taken to protect council systems and information from threats distributed via internet and email.

Staff who use council IT systems will be responsible for reporting any suspected incidents of computer virus infection to the IT Help Desk for further assessment and rectification.

14. DATA BACK-UP

Adequate backup facilities will be provided to ensure that all essential business information can be backed up and recovered if necessary.

Backups and accurate and complete records of backup copies should be stored in a remote location, sufficient to escape any damage from a disaster at the main site.

15. FAULT LOGGING

Faults in IT systems will be reported to the council's IT Help desk where they will be processed in accordance with the help desk procedures.

Only persons authorised by the Service Manager Digital Enablement and IT will carry out repairs and servicing of council equipment.

16. NETWORK MANAGEMENT

The council's data networks will be managed in such a way as to prevent unauthorised logical and physical connection, and to detect unauthorised connection should this occur.

No connection to the council's communications network will be permitted without the prior approval of the Service Manager Digital Enablement and IT.

17. MEDIA HANDLING AND SECURITY

To prevent the possibility of damage, theft or unauthorised access to council information assets and interruptions to business activities, all systems or media containing data will be stored securely.

18. SYSTEM ACCESS CONTROL

Angus Council will restrict access to information systems to only those staff and authorised agents of the council who require such access to enable them to undertake their duties.

It is the responsibility of all Heads of Service, and the Service Manager Digital Enablement and IT to implement this policy as required.

Access controls and the use and protection of passwords is set out in the "Information Security User Guidelines". These guidelines will be made available to all users of council information systems.

The installation and upgrade of operational systems will only be performed by arrangement with the Service Manager Digital Enablement and IT.

19. BUSINESS CONTINUITY PLANNING

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures and disasters, appropriate directorate/services business continuity management processes will be implemented.

20 COMPLIANCE

The Council's Leadership Team will implement appropriate procedures to ensure that all procurement of IT systems conforms to appropriate legislative requirements in addition to the council's Standing Orders and Financial Regulations.

System owners shall ensure that important council records will be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements as well as to support essential business activities.

20. DATA PROTECTION

Applications and systems handling personal data as defined under the General Data Protection Regulations will comply with the legislation and its principles.

21. PREVENTION OF MISUSE OF IT FACILITIES

The council's information processing facilities are provided for business purposes. The use of information processing facilities will be authorised by the appropriate service owner.

If any misuse is identified it will be subject to the appropriate disciplinary action.

22. COMPLIANCE WITH SECURITY POLICY

All areas within the organisation will be regularly reviewed to ensure compliance with security policies and standards.

The Council's Leadership Team will ensure that all security procedures within their area of responsibility are carried out correctly.

23. SYSTEM AUDIT CONSIDERATIONS AND CONTROLS

Periodic audits of working practices will be undertaken to ensure compliance with this Information Technology (IT) Security Policy.

System owners will arrange a continual review of operational information systems to ensure that security controls have been properly implemented and continue to be effective.