IT SECURITY POLICY

INTRODUCTION

The objective of Tayside Contracts IT Security Policy is to protect Tayside Contracts' computerised information assets from all threats whether internal, external, accidental or deliberate to ensure;

- Continuity of operation of Tayside Contracts communication and information systems.
- Reduction of the risks of damage from any security incident.

The principles of information security provide the framework that ensures the protection of all information within Tayside Contracts. These are;

Confidentiality:	Protection of information from unauthorised disclosure.
Integrity:	Safeguarding the accuracy and completeness of information.
Availability:	Ensuring that information and associated services are available to users when required.

Only those persons authorised by the Managing Director of Tayside Contracts are permitted access to information systems. All information held is for authorised Tayside Contracts business only.

SCOPE OF POLICY

This policy applies to all employees of Tayside Contracts, to third party organisations or contractors and to anyone else who is authorised to access and use Tayside Contracts ICT facilities, systems or services.

This policy applies to all electronic media and data held by Tayside Contracts, and includes data stored on; databases, disks, tapes, USB drives, CD's, DVD's, films, videos and voice used to convey, store, manage or process information, knowledge and ideas;

- Accessed on or from any Tayside Contracts premises;
- Accessed using Tayside Contracts computer equipment;
- Accessed from an individual's own devices, remotely or by wireless within the premises, and/or used in a manner that identifies the individual with Tayside Contracts.

LEGAL FRAMEWORK

All systems operated by Tayside Contracts are subject to the General Data Protection Regulation 2018, Data Protection Act 2018, Computer Misuse Act 1990, Copyright Patents and Designs Act 1988 and other legislation and guidelines as may be issued from time to time to regulate the use of information systems. Checks may be carried out to ensure compliance with legislation.

SECURITY INCIDENTS

A security incident is defined as any event such as a security breach, threat, weakness or malfunction that has, or could have resulted in the loss or damage to Tayside Contracts information assets.

This can also include events such as power cuts or non-availability of communication systems. If in doubt, the incident should be reported. Any suspected security incidents should be reported to the Organisational Development Manager (01382 834114 / gdpr@tayside-contracts.co.uk) and/or the IT Manager (01382 834007) via telephone or email as soon as possible.

DISCLOSURE OF INFORMATION

Disclosure of information may take many forms, including viewing records on PC's, laptops or terminals, email or typewritten correspondence, computer printouts, photocopying, by word of mouth or mobile/landline telephone conversation.

If you are unsure about a request from a colleague or other person to disclose information it is your duty to refer it to your line manager prior to disclosure.

Any requests made to managers for personal data relating to an employee e.g. address details, salary details etc should be directed to the HR Admin team for processing via the correct protocol.

SECURING WORKSTATIONS

All users should close documents prior to locking or logging out of their computer workstation (PC, laptop or thin client terminal).

On leaving the workstation users must either log out or lock it by using the CTRL+ALT+DELETE keys then select "Lock Computer".

Users are encouraged to use a built-in screensaver wherever possible and to adjust the settings to enforce the use of a password to return to the desktop on activation of the screensaver.

To log out at the end of the working day users must log out of and shut down their computer workstation using the "Start, Shut Down" (PC or Laptop) or "Start, Log Off <username>" (Windows Terminal). After following either procedure the monitor should be switched off.

DATA STORAGE

All authorised Tayside Contracts users will be allocated a number of drive mappings to be used for storing and sharing documents and other data. An "F" drive will be mapped by default which provides a personal folder on the server to which only the user will have access. Other drive mappings will be allocated based on job role and function and these will be shared drives to which other users within similar job roles or organisational units may also have access.

Users must take extra care when making use of shared drives to ensure that only business relevant documents are saved and that data of a sensitive nature is only saved in shared drives where appropriate – eg employee details may be saved within a drive shared by nominated members of the HR Unit, all of whom may require to access it as part of their job role. Care must also be taken when deleting or moving files in shared drives to ensure that other user's files or folders are not accidentally deleted or moved.

Users are encouraged not to store their own personal data (documents, photo's etc) in F drives but Tayside Contracts will tolerate reasonable use of personal storage up to a limit of 100Mb. Checks may be carried out to ensure compliance with this and users with excessive amounts of personal data may be required to delete files to recover disk space.

ACCESS AUTHORISATION

Only trained and authorised personnel will be granted access to Tayside Contracts IT information systems. The level of access granted will be commensurate with the post and requests for access to additional systems will be made to your Line Manager in the first instance as will requests for systems training.

Access to network resources and drives is granted based on job function and operational requirements. Access to additional network drive letters / specific folders must be requested by a line manager using the IT Helpdesk Portal (http://grandpaw:9675/portal/).

Under no circumstances will access to additional network drives be granted without this form completed and authorised by the relevant manager. Access to another users personal folder (F drive) can only be authorised by the Managing Director or his nominated deputy and will only be granted in the event of an operational emergency or as part of an investigation into serious misconduct.

IT information systems should not be used for personal purposes and users must only access information for which they are authorised. Browsing of electronic systems without authorisation is not permitted.

It is expressly forbidden to allow another person to use your login/password to access the system or any application. All users are personally accountable for all actions carried out under their login and password.

PASSWORDS

Access to all Tayside Contracts corporate systems is governed by strict username/password controls. Passwords must adhere to basic guidelines and should not be documented or divulged to others.

All Tayside Contracts systems are password protected from unauthorised use. Each user has an Active Directory (AD) account which, by use of individual user profiles allows access to software and corporate systems as appropriate to their job function. Please refer to Appendix 1 which details password criteria and complexity rules.

Access to software systems such as Integra, Snowdrop and FleetWave are also subject to strict password control although to a lesser extent than AD accounts. Users will be asked to change their passwords at least once per year using the same password complexity noted

above. Users must not use “password” or their username and must ensure that passwords are not the same as that used for Active Directory access.

UNAUTHORISED SOFTWARE

Only software authorised by the IT Manager and installed by members of the IT Unit is allowed to be used by Tayside Contracts employees. No software, including evaluation, freeware, shareware or games shall be installed on any PC, laptop or server unless by a member of IT staff and in strict adherence to any associated licensing restrictions.

All requests for software must be made to the IT Manager in the first instance.

COMPUTER VIRUSES

Centrally installed and monitored anti-virus software in installed throughout Tayside Contracts to prevent virus attacks on systems. In the event that a virus is suspected users should adhere to the following;

- Contact the IT Unit immediately.
- Note the symptoms and any message appearing on the screen.
- Stop using the computer and where possible remove the network cable or switch off.
- Do not use disks or USB attached drives from the computer on any other computer.
- Do not attempt to remove suspected software unless instructed to by a member of the IT Unit.

BACKUPS

Backup procedures are in place for all centrally stored network data and whilst these will not prevent errors or losses they will help ensure that when something goes wrong or data is deleted, recovery is possible.

Users should note that there is no automated process in place to backup laptop or PC data stored on local hard drives (C drives). Sensitive or important data should always be saved to a network drive (F, G etc) to ensure that files are secure and backed up. Laptop users should copy any files created offline to a suitable network drive as soon as possible once reconnected to the network. It is the responsibility of the user to ensure that data is saved in a location that can be backed up.

END POINT / USB STORAGE DEVICES

End point data storage devices cover the storage of data on devices that can be connected either by USB, data cable or by wireless connection direct to any computing equipment within Tayside Contracts.

Tayside Contracts does not permit the use of unauthorised and unencrypted USB removable storage devices and will supply approved data storage devices for business purposes. It is the users responsibility and obligation to ensure that all end point data devices, where approved for use, are used only for their intended business purpose and that information contained or transmitted via these resources are protected from unauthorised use, copying or modification for personal advantage.

SECURITY AND MOVEMENT OF EQUIPMENT
IT equipment must only be moved by, or under guidance from, IT Unit staff.

SECURITY OF EQUIPMENT OFF PREMISES
IT equipment, regardless of ownership, used outside Tayside Contracts premises to support business activities, must be afforded the equivalent level of protection to that of on-site equipment.

- Procedures and controls as detailed within this document must be adhered to and applied to IT equipment used away from Tayside Contacts' premises.
- When travelling, IT equipment and media (including CD's, DVD's and USB pen drives) must not be left unattended.
- Laptops must be carried as hand baggage when travelling.
- IT equipment, (including mobile telephones) must always be removed from vehicles which are left unattended.

REMOTE ACCESS
Access to Tayside Contracts IT resources from out-with the network can be achieved using a secure VPN connection through our corporate firewall. This requires internet access and software to be installed on a PC or laptop.

Remote access will only be granted following a valid request by a line manager using the form on the IT Helpdesk Portal (http://grandpaw:9675/portal/).

This form must also to be used for external contractors and consultants prior to connection to Tayside Contracts network and must be approved and authorised by the IT Manager and Head of Division/Unit prior to access being granted.

Where authority has been granted to access Tayside Contracts' network remotely, users will be issued a secure username/password along with the necessary VPN (Virtual Private Networking) software to allow connection. Remote connection to Tayside Contracts network requires a connection to the internet which is the responsibility of the user if it is their own private or public broadband equipment.

Under no circumstances will a connection be made using Cisco AnyConnect VPN from a PC or laptop which has not been issued by Tayside Contracts IT Unit.

Laptops issued by Tayside Contracts will have hard disk encryption enabled, fully up-to-date anti-virus and firewall software installed and the necessary software to allow a secure VPN connection to the network. The use of home PC's or laptops is not permitted when using this connection method.

Accessing corporate systems and email from remote locations carries further security risks and threats and users are encouraged to adopt greater awareness when away from Tayside Contracts' formal network environment.

When using a laptop remotely, always consider whether the on screen data may be overlooked or your password compromised i.e. at home, on a train or in a public area.

Particular attention should be paid to the guidelines for securing workstations, as detailed in Section 6 of this document when accessing the network remotely. The laptop or PC should be logged out when not in use and connection to the network terminated.

POLICY VIOLATIONS

Failure to comply with the terms and conditions of this policy may be regarded as misconduct and will be addressed in accordance with Tayside Contracts' Disciplinary Policy.

RELATED POLICIES

The IT Security Policy links to the following policies which can be accessed on the Intranet, or requested from your line manager or from the HR Admin Team:

- Grievance Policy
- Disciplinary Policy
- Equality and Diversity Policy
- Acceptable Use of Social Media Policy
- Employee Code of Conduct
- Data Protection Policy
- Data Breach Management Procedure

POLICY REVIEW

The IT Security Policy will be reviewed every 3 years or sooner if required by legislative or operational changes.

Should you have any queries or require further clarification regarding any aspects of this policy please contact the IT Manager on 01382 834007 or helpdesk@tayside-contracts.co.uk

APPENDIX 1

PASSWORDS

Users may choose their own password but it must meet the following enforced criteria;

Minimum Password Length: 8 characters
Maximum Password Age: 6 Months
Minimum Password Age: 1 day
Password History: 10 passwords remembered
Password Complexity: Passwords must meet the following minimum requirements:

- Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Be at least six characters in length.
- Contain characters from three of the following four categories:
  English uppercase characters (A through Z)
  English lowercase characters (a through z)
  Base 10 digits (0 through 9)
  Non-alphabetic characters (for example, !, $, #, %)

Complexity rules will enforce that user passwords cannot be the word "password" or be the same as their username. Passwords cannot be re-used until the password history period has

been exceeded and should be changed immediately if compromised. Passwords should not be divulged to any other person unless requested by a member of IT staff to allow troubleshooting or other user assistance.