BON ACCORD

ABERDEEN
CITY COUNCIL

CORPORATE
ICT ACCESS CONTROL POLICY

Date:	23 January 2019	
Version:	V0.6	
Location:	Digital & Technology	
Author (s) of Document:	Lita Greenwell, Information Security Officer	
Approval Authority	Audit, Risk & Scrutiny	
Scheduled Review:	March 2020	
Changes:	N/A	

1. What is this policy for?

This policy defines the Council's rules necessary to maintain an adequate level of security and protection for Council information, data, hardware, systems/applications and any other ICT resources from unauthorised access, while ensuring their secure and reliable operation.

For the avoidance of doubt, system(s)/application(s) refers to any Council administered/hosted/licensed software, digital resources, networks, servers and other infrastructure, and communication channels, and includes the data carried and stored thereon. Hardware includes, but is not limited to, laptops, notebooks, tablets, desktop computers, mobile telephones, smart phones, telephones, printers and other peripherals, tills, kiosks, and storage media.

2. Who is this policy for?

This policy applies to all staff, agency staff, elected members, contractors and sub-contractors, and to any person, without exception, who manages, administrates, uses or requires access to Council information, systems and/or applications.

3. Why do we need this policy?

All Aberdeen City Council information is valuable, and protecting it from unauthorised access is vital. Having an ICT Access Control Policy in place helps the Council to mitigate information security risks. It enables system/application administrators to establish procedures to manage and control access to Council information, in line with agreed, corporate principles and legislation.

It also gives standards and minimum requirements for the access control of new or upgraded systems/applications to adhere to ahead of them gaining approval for purchase and/or implementation. These standards and requirements are based on legislation and industry good-practice. By securing ICT access before systems/applications are installed, we can streamline the deployment of new technologies. The Council is required under Data Protection legislation to be able to evidence a 'Data Protection by Design and Default' approach to protecting personal data, and ensure that personal data is "processed in a manner that ensures appropriate security of the personal data […] using appropriate technical or organisational measures". Adopting and implementing this Access Control Policy is a key component of the Council being able to comply with these requirements.

4. What does it mean for the Council? (Policy Statement)

4.1 What is Access Control?

Access control is the restriction of people's access to a resource. In ICT, this means that you can only use a digital resource, such as a laptop, digital information or a program, if you have been granted permission to access it. This helps us protect our information assets and systems from intentional or accidental compromise, whether through malicious software (or malware, such as viruses or trojan horses), security attack, modifications or access to confidential or protected information. These controls are applied to user accounts, accounts used by automated or work-flowed processes, and to systems and programs.

For information on securing hardcopy information, buildings and devices, see the Corporate Information Handbook (Section 7). For information on access to CCTV Systems, see the CCTV Procedure.

4.1.1 Principle of Least Privilege

Access to all Council information and digital assets should be on a need-to-know basis only. Therefore, all accounts must adhere to the Principle of Least Privilege (PoLP). Essentially, this means that access to information is restricted in 2 ways:

1. You can only see the information you need to do your job
2. What you can do with that information is restricted to what you need to do to fulfil your duties

For example, only you, your line manager, Payroll and Organisational Development need access to parts of your HR data, depending on their role. Your line manager doesn't need access to your banking details, Payroll only need to read your banking details, and only you need access to update them.

Not only does PoLP improve information security, it also assures better system stability as limiting access makes it easier to identify and test the possible actions an account can carry out, and the affects that these actions could have on other users, processes and systems. This therefore makes it easier to design and receive approval to deploy a system.

4.2 System/Application Requirements

Some system and application default installations can present weak points in our ICT landscape that can easily be exploited. To prevent this, some simple controls can improve our protection:

- Any user accessing Council ICT systems/applications must be authenticated with a minimum of single-factor authentication, usually comprising a unique identifier (such as a username) and a password. Where it has been implemented, users may be asked to authenticate with multi-factor authentication which requires additional credentials, such as a pin or logging on from a registered device.
- Any account password requirements (length, complexity, etc.) must adhere to the Council's Password Standard [add link] and the guidance outlined in Section 4.4 below.
- Any network or system initial-login page should carry a disclosure notice warning users that only those authorised to do so should access the system.
- Logs must be maintained of any inbound access, both granted and denied, to the Council's internal network by any users or systems outside of the network.
- All Council workstations (desktop, laptop, tablet, etc.) must use approved single-factor authentication, and have password enabled screen locks and time-out after a period of inactivity (no more than 10 minutes), unless an approved exception (such as public access machines, kiosks and some education tablets).

- Local workstation administrator accounts should be unique, and user access to them prohibited.
- Access controls must be applied to all digital information assets to ensure that they are only accessed by those who need to have access, and that they are not incorrectly shared, changed, deleted or made unavailable in any way.
- Systems/applications should keep logs of actions carried out by users and administrators for audit purposes, as appropriate for the type of data they capture, and these logs should not be accessible by unauthorised users or be editable in any way. Logged actions must be able to be traced back to a specific user account. Where a system contains sufficiently sensitive information, audit trails and logs must be backed up and stored in accordance with the Corporate Records Retention & Disposal Schedule.
- User passwords for systems/applications must never be stored in unprotected, plain-text format.
- Any system/application auto-run features which allow file execution without user authorisation must be disabled.

4.3 Creating, Controlling and Managing Accounts

All systems and applications require a documented security matrix, detailing account types and their capabilities no matter the access control system employed. Ideally, they will also detail the anticipated PoLP level required for Council functions or users, based on job role, to complete their duties. This matrix will facilitate any review or audit of systems/applications and speed up the deployment of new systems/applications.

All accounts must be created in such a way that the identity of the account user can be established at any time, by any administrator.

Accounts must only be created or have their access or capabilities elevated with correct approval, such as from the system owner, the Information Asset Owner (IAO) or senior management. This approvals process must be documented and agreed ahead of system/application deployment.

Accounts should only be kept active for as long as they are required, and a process to manage leavers and transfers (such as promotions, secondments and redeployments) must be in place. Unnecessary or inactive accounts **must** be disabled and/or removed as soon as possible or practicable. Accounts must be disabled and/or removed when notification to do so is received as part of the Managing Leavers Process.

Procedures should be in place to establish a user's identity before providing them with a new, replacement or temporary password. It is insufficient for them to provide, for example, only their username (as this is visible to anyone who may encounter a locked Council workstation).

New or replacement passwords issued by ICT or other system support teams must be changed at first login.

Administrator accounts should not be used for day-to-day activities and should only be used where admin privileges are required to complete the task. Administrators should use a standard account for normal activities.

Administrator accounts should be unique, have a different password from the user's standard account and never be shared.

New accounts must not be created as a replica of another account, mirroring its access and/or permissions.

Third-party account requests must come through the ICT Service Desk and their access must be logged and time restricted. Any extension to their accounts must be reviewed on a case-by-case basis and appropriately logged.

4.4 Password Creation & Management

Passwords must meet the Council's Password Standard [link].

Personal passwords must never be re-used as work passwords.

Passwords must never be shared (see the ICT Acceptable Use Policy). If a user thinks their password has been inadvertently disclosed, then they must change it to a new password that doesn't resemble their old password (i.e. don't just change a number or character) and that meets the requirements of this policy.

Any default, vendor-supplied or easily guessable passwords must be changed to something non-obvious and in accordance with the requirements of this policy and the Password Standard.

Where the technical controls are available, systems containing Council data or information must be password protected. Where possible, and reasonably practicable, single-sign-on or password synchronisation should be implemented.

To protect against brute-force password guessing, accounts must lock after no more than 10 unsuccessful attempts, or they must limit the number of attempts allowed within a given period.

5. Roles & Responsibilities

Everyone who uses and accesses the Council's ICT resources must do so in accordance with this policy and all related corporate policies, and corporate and local procedures (see section 9 below). Any breach or deviation from this policy must be raised through the Information Security Incident Reporting Procedure (ISIRP) and investigated accordingly. In addition to this, the below groups have additional responsibilities.

5.1 Users

All users must read, understand and agree to comply with this policy, the ICT Acceptable Use Policy, the Corporate Information Policy and any other related or supporting policies and procedures.

All users should undertake any required or recommended corporate or local training, and follow any available guidance, on accessing and using Council information and digital resources.

Users must only access the information they need to do their jobs. Users must notify the ICT ServiceDesk via ServiceNow if they have access to a system or shared drive, or to an area of a system or shared drive, that they shouldn't have. This access will then be removed.

Users must secure information properly and in line with all pertinent information policies, thereby ensuring that only those who need access to the information will be able to access it, as outlined in your responsibilities regarding information and confidentiality in the Employee Code of Conduct and the Councillor Code of Conduct.

5.2 Managers

Managers should ensure that their team members are aware of this and all related policies, and that they and their team have undertaken any necessary training.

Managers must follow the new start and leavers processes, and ensure that new users', role changers', transfers' (e.g. secondments or redeployments) and leavers' access requests are submitted and processed promptly.

5.3 Information Asset Owners

Information Asset Owners (IAOs) are senior business managers who are responsible and accountable for the specific, defined information assets within their remit, in accordance with the Council's Information Asset Owner Handbook. This includes digital information resources, such as laptops, mobile devices, tablets, etc. They are responsible for ensuring:

- All staff understand and act in accordance with their responsibilities outlined in this policy.
- Security matrices are in place, fit for purpose and are being used for the information assets under their remit.
- User account creation, control and management procedures for the information assets under their remit are in place and adhere to this policy.
- Guidance and training are available to safeguard the secure and safe use of the information assets under their remit.
- System administrator accounts are suitably limited and controlled for the information assets under their remit.

5.4 System Administrators & Privileged Users

System administrators and privileged users have significant, additional capabilities when working with digital resources, and are authorised to perform system- and security-related functions that ordinary users are not authorized to perform. Examples of system- and security-related functions include starting/stopping application services, creating/updating other user accounts, etc. For this reason, administrator accounts come with additional responsibilities and require stronger passwords.

Compromise of some administrator accounts could be a threat to the whole organisation, giving hackers or other hostile actors access to our whole network and everything within it. As a result, users of these accounts have additional responsibilities and they:

- Must keep an up-to-date security matrix for each system they administrate.

- Must document the user account creation, control and management procedures for each system they administrate and in accordance with this policy.
- Must maintain audit logs of access requests and changes to systems/applications that they are responsible for.
- Must only use their administrator accounts to carry out administrator responsibilities. Day-to-day, regular user responsibilities should be carried out using a standard, PoLP user-account.
- Must never use their administrator accounts to access the internet.
- Must remove system administrator account access from areas of a system/application if requested to by the IAO or a senior manager acting as request approver. In these cases, access can only be added again, with the necessary approvals, for a defined period to carry out specified, administrative tasks.
- Must seek clarity and, if deemed necessary, additional approval if they receive a request for a user account with unusually broad/deep privileges that do not match the security matrix.
- Must not use their access to elevate their privilege without the necessary approvals.
- Must not amend any system/application logs or audit trails.
- Must only use a system administrator account from a Council device.

5.5 ICT Security Team

As the owners of this policy and subject matter experts in ICT and information security, the ICT Security Team will provide guidance on any aspect of this and related policies and procedures, or direct users to the most appropriate team.

6. How will we know if it’s working?

Any breaches or deviation from this policy will be reported via the Information Security Information Reporting Procedure, and they will be investigated accordingly. These will then be reported in the Information Governance Management Quarterly Performance Report, and by the Council’s Senior Information Risk Owner (SIRO) to the Corporate Management Team, as required.

7. How will we manage any risks that affect this policy?

7.1 Cluster Risk Registers

Information Asset Owners are responsible for managing risk to the information assets that they are responsible for; these risks are managed through Cluster Risk Registers and are included in Business Continuity planning and disaster recovery arrangements wherever appropriate.

7.2 Corporate Risk Register

Information Governance and Cyber Security also pose a strategic risk for the Council. The relevant Corporate Risk Owners provide the Council’s Corporate Management Team with regular updates on the strength of controls in place against this risk.

8. How will we make sure this policy is kept up to date?

This Policy will be reviewed annually by the Council's Information Security Officer to ensure that it meets business and accountability requirements and measurable standards of good practice.

9. Related Policy Document Suite

- Corporate Information Policy
- ICT Acceptable Use Policy
- Employee Code of Conduct (for Employees only)
- Corporate Protective Monitoring Policy
- Councillors Code of Conduct (for Elected Members only)

Procedure

- Corporate Information Handbook
- Information Security Incident Reporting Procedure
- Requesting Access to Information Procedure
- Information Asset Owner Handbook
- Third Party Access
- Managing Leavers Process Guidance
- CCTV Procedure

Standard

- Password Standard [link]

Related Legislation

- The Data Protection Act 2018
- General Data Protection Regulation
- The Public Records (Scotland) Act 2011
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Regulation of Investigatory Powers (Scotland) Act 2000