ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk & Scrutiny
DATE	14/01/2019
REPORT TITLE	ICT Access Control Policy
REPORT NUMBER	CUS/19/161
DIRECTOR	Andy MacDonald
CHIEF OFFICER	Andrew Howe
REPORT AUTHOR	Lita Greenwell
TERMS OF REFERENCE	Section 11 – Audit, Risk and Scrutiny Committee, Purpose 1.1 and Remit 1.4

1. PURPOSE OF REPORT

To seek Committee approval of the ICT Access Control Policy.

2. RECOMMENDATION(S)

That the Committee:

2.1 Approve the ICT Access Control Policy as outlined below and at Appendix 1.

3. BACKGROUND

3.1 The Council's Digital Transformation Programme is embracing technology and introducing new systems to improve the day-to-day delivery of Council services. Good governance is needed to ensure that these new systems and technologies can be deployed smoothly and securely, protecting our customers' and employees' information. By not properly securing this information, we not only risk personal data breaches for which we could incur maximum fines under GDPR of 4% of turnover, or €20 million, whichever is higher, but we could also find ourselves open to compensation action from data subjects.

3.2 A Financial Systems Audit Report (draft) produced by KPMG highlights a risk where "privileged user access is not robustly controlled", increasing the risk to

Council information assets. A recommendation was made that a formal policy be established that "guides the Council's management of highly privileged access". This policy meets this recommendation.

3.3 Implementation of this policy will consist of an all-staff awareness exercise, and procedure updates and creations, with assistance from ICT Security as required, to ensure compliance with this policy:

a. Liaise with the Internal Communication team on an all-staff awareness exercise, and focussed communications to Information Asset Owners and Systems Owners.
b. The project management procedures within Digital and Technology will be updated to include ICT Security requirements, which adhere to this policy, in the requirements-gathering phase and in the tender process for all new-software projects, and for projects moving applications to the Cloud.
c. Digital and Technology procedures and guidance will be updated.
d. System administrator and elevated user procedures will be updated in each Service that manages their own software.
e. Recommendation will be made to update all user guidance, as necessary/appropriate.
f. New Start Checklist will be updated to ensure new employees have read and understood their roles and responsibilities with respect of this policy,

4. FINANCIAL IMPLICATIONS

4.1 There are no additional financial implications as a result of this policy. All security requirements will be included within the tender documentation, as already happens for requirements collated with input from the ICT Security Team. This will also prevent possible future costs of upgrading or purchasing new systems without recourse to the requirements of this policy.

5. LEGAL IMPLICATIONS

5.1 Adoption of the ICT Access Control Policy will strengthen the Council's compliance with data protection legislation (GDPR and the Data Protection Act 2018) which requires that we are able to evidence 'Data Protection by Design and Default' and ensure that personal data is "processed in a manner that ensures appropriate security of the personal data […] using appropriate technical or organisational measures".

5.2 The Computer Misuse Act 1990 disallows unauthorised access or acts in relation to computer systems, data or materials, and the ICT Access Control Policy aims to prevent this through the appropriate management of access to Council information, data, hardware, systems/applications and any other ICT resources.

6. MANAGEMENT OF RISK

	Risk	Low (L), Medium (M), High (H)	Mitigation
Financial	Non-compliance with applicable legislation (see Section 5 above) may lead to enforcement action with monetary penalties and/or financial liability for damages to customers.	M	The Council's wider Information Assurance framework mitigates against the risk of non-compliance – training, incident processes, associated policies, monitoring and reporting.
Legal	Non-compliance with applicable legislation (see Section 5 above) may lead to enforcement action.	M	The Council's wider Information Assurance framework mitigates against the risk of non-compliance – training, incident processes, associated policies, monitoring and reporting.
Employee	For some users with elevated privilege (such as System Administrators) there is a risk of non-compliance with the policy as it represents a change in current practice.	L	If approved, the policy will be supported by appropriate awareness activities and suitable guidance and assistance in helping these users create new procedures, as required.
Customer	Customers at risk of harm due to inadequate security and management of personal data.	M	This policy, along with the Council's wider Information Assurance framework, mitigates against this risk by ensuring 'Data Protection by Design and Default'.
Environment	No Risks		
Technology	Cyber security of the Council's environment is at risk from users with elevated privilege using their administrator accounts online.	M	If approved, this policy, supported by appropriate awareness activities and suitable guidance, will mitigate this risk.
Reputational	Realisation of any of the above risks would likely lead to reputational	H	Implementation of the above mitigations will reduce the risk of reputational damage.

	damage to the Council.		

7. OUTCOMES

Local Outcome Improvement Plan Themes	
	Impact of Report
Prosperous People	This policy, along with the Council's wider Information Assurance framework will reduce our customers' risk of harm due to inadequate security and management of personal data.
Enabling Technology	Information and data are key assets of the Council, and securing the technologies that enable the transmission, storage and processing of this data forms part of the Council's wider Information Assurance framework, to ensure our information is fit to enable the Council to deliver outcomes for our people, place and economy.

Design Principles of Target Operating Model	
	Impact of Report
Customer Service Design	By implementing the ICT Access Control Policy, we will be assuring security and privacy of all data while supporting the principle of "Being Digital"
Workforce	By implementing the ICT Access Control Policy, we will be assuring the security of all data in the cloud, enabling our workforce to be flexible and agile, working securely from anywhere.
Process Design	By implementing the ICT Access Control Policy, we will be assuring security and privacy be design for the applications/systems supporting new/redesigned processes.
Technology	By implementing the ICT Access Control Policy, we will be assuring the security of all data in the cloud, enabling our workforce to work securely from anywhere.

8. IMPACT ASSESSMENTS

Assessment	**Outcome**
Equality & Human Rights Impact Assessment	EHRIA required
Data Protection Impact Assessment	Not required
Duty of Due Regard /	Not applicable

Fairer Scotland Duty	

9. BACKGROUND PAPERS

Not applicable

10. APPENDICES (if applicable)

Appendix 1: ICT Access Control Policy
Appendix 2: Password Standard

11. REPORT AUTHOR CONTACT DETAILS

Lita Greenwell
Information Security Officer
lgreenwell@aberdeencity.gov.uk
01224 523857