East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 20 June 2017

BY: Depute Chief Executive (Resources & People Services)

SUBJECT: Internal Audit Report – Information Security

---

1 PURPOSE

1.1 To inform the Audit and Governance Committee of the recently issued audit report on Information Security.

2 RECOMMENDATION

2.1 That the Audit and Governance Committee note the contents of the Executive Summary and Action Plan.

3 BACKGROUND

3.1 A review of the internal controls surrounding Information Security was undertaken as part of the Audit Plan for 2016/17.

3.2 The main objective of the audit was to ensure that the internal controls in place were operating effectively.

3.3 The main findings from our audit work are outlined in the attached report.

4 POLICY IMPLICATIONS

4.1 None

5 INTEGRATED IMPACT ASSESSMENT

5.1 The subject of this report does not affect the wellbeing of the community or have a significant impact on equality, the environment or economy.

6 RESOURCE IMPLICATIONS

6.1 Financial - None

6.2 Personnel - None

6.3 Other - None

7 BACKGROUND PAPERS

7.1 None

AUTHOR'S NAME	Mala Garden
DESIGNATION	Internal Audit Manager
CONTACT INFO	01620 827326
DATE	8 June 2017

EAST LOTHIAN COUNCIL – INTERNAL AUDIT
INFORMATION SECURITY

1. EXECUTIVE SUMMARY

1.1 Introduction

As part of the Audit Plan for 2016/17 a review was undertaken of the Information Security arrangements in place within the Council. A summary of our main findings is outlined below.

1.2 Areas where Expected Controls were Met

- A high level Information Security Policy is in place setting out the Council's commitment to Information Security.
- Adequate arrangements are in place to ensure that user access to the Council's corporate network is properly controlled.

1.3 Areas with Scope for Improvement

- There was a failure to ensure that information security standards, procedures and guidance documents were readily available to employees on the Council's intranet. *Risk – lack of awareness of information security procedures.*
- For employees moving to another position within the Council, there was a lack of effective processes in place for managing user access to individual systems. *Risk – employees may have access to confidential or sensitive information that they no longer require.*
- There was a failure to ensure that an up to date record was maintained of portable IT equipment – in a number of cases, laptops were recorded as being allocated to former employees of the Council and in some cases laptops allocated to former employees could not be located. *Risk – loss or misuse of Council assets or information.*
- The procedures in place for ensuring laptops are checked and updated on a regular basis require review. *Risk – failure to ensure laptops receive automatic updates.*
- At present, there is a lack of adequate monitoring arrangements in place for identifying and suppressing inactive user accounts. *Risk – failure to ensure that systems access is restricted.*
- There was a failure to ensure that all relevant employees had undertaken the mandatory information security training. *Risk – lack of awareness of information security procedures.*

1.4 Summary

Our review of the Information Security arrangements in place within the Council has identified a number of areas with scope for improvement. Detailed findings and recommendations are contained in our main audit report.

Mala Garden
Internal Audit Manager **June 2017**

EAST LOTHIAN COUNCIL – INTERNAL AUDIT
INFORMATION SECURITY

ACTION PLAN

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.2.2	Management should ensure that all information security standards, procedures and guidance documents are readily available to employees on the Council's intranet. Management should ensure that a clear link is provided to the IT policy documents that are located within the IT Service Desk section of the intranet.	Medium	Service Manager IT Infrastructure	Accepted – we will look to revise the content of the IT pages on the Intranet to ensure they hold key policy documents.		August 2017
3.3.2	Management should ensure that a properly authorised user access request form is in place for all users of individual systems. Management should ensure that all changes to users' access levels are properly authorised by their line manager. Evidence of the authorisation should be retained on file.	Medium	Systems Administrators – Corporate	Agreed		June 2017
3.3.3	Management should ensure that users with access to sensitive and confidential information have signed the most up to date user access request form confirming that they have read and agree to abide by the conditions of use.	Medium	Systems Administrator – MOSAIC	Agreed – all users will be asked to sign and return the MOSAIC access form.		June 2017

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.3.4	Management should ensure that regular monitoring of inactive user accounts is undertaken – user accounts that have been inactive for a specific period of time should be suppressed.	Medium	Systems Administrators – Corporate	Agreed		August 2017
3.3.5	Management should ensure that appropriate arrangements are in place to notify all relevant parties of employees removed from the Council's Payroll system following the annual review.	Medium	Payroll Manager	Agreed		In place
3.3.6	Management should ensure that details of agency workers whose network access has been revoked are passed to the local systems administrators.	Medium	Service Manager IT Infrastructure	Accepted – requires discussion with HR and service areas to agree a procedure.		December 2017
	Management should ensure that for temporary workers and agency staff the user access request forms provide an end date to ensure that access is revoked timeously.		Systems Administrators – Corporate	Agreed		July 2017

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.3.7	**Management should review the arrangements in place for informing local systems administrators of employees who move to another position within the Council.**	**Medium**	**Depute Chief Executive – Resources and People Services on behalf of CMT**	**Agreed – information note to be sent to Heads of Service and Service Managers.**		**July 2017**
3.4.1	**Management should ensure that the existing leavers' notification circulation list includes staff with responsibility for maintaining the asset management database.**	**Medium**	**Service Manager IT Business Services**	**Accepted**		**June 2017**
	Management should review the current arrangements in place for maintaining the asset management database to ensure that information held is accurate and complete.		**Service Manager IT Business Services**	**Accepted**		**December 2017**
	Management should ensure that a designated member of staff is identified within each service area with responsibility for maintaining an up to date record of all laptops assigned to the service area – the Council's IT section should be notified of the designated member of staff.		**Depute Chief Executive – Resources and People Services on behalf of CMT**	**Agreed – information note to be sent to Heads of Service and Service Managers.**		**July 2017**

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.4.1 (cont)	**Management should ensure that adequate procedures are in place for laptops to be checked and updated on a regular basis.**	**Medium**	**Service Manager IT Business Services / Service Manager IT Infrastructure**	**Accepted – revising checking procedures and ensuring unused devices are disabled from the network after 3 months. Longer term we will investigate an Access Control system.**		**December 2017**
3.5.1	**Management should ensure that the Information Security Incident Management Procedures are updated to reflect the current arrangements within the Council – the procedures should be made available on the Council's intranet.**	**Medium**	**Service Manager IT infrastructure**	**Accepted – will update procedures and publish on the intranet.**		**August 2017**
3.6.1	**Management should give consideration to developing an Information Classification and Handling Procedure.**	**Medium**	**Service Manager – Licensing, Admin and Democratic Services**	**Agreed – full consideration will be given to the implications of adopting a classification scheme.**		**June 2018**

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.7.1	**Management should ensure that information security training is undertaken by all relevant employees.**	**Medium**	**Team Leader – Infrastructure and Security**	**Agreed – regular reports on training will be obtained and reminders will be sent to service areas.**		**October 2017**

Grading of Recommendations

In order to assist Management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
High	Recommendations which are fundamental to the system and upon which Management should take immediate action.
Medium	Recommendations which will improve the efficiency and effectiveness of the existing controls.
Low	Recommendations concerning minor issues that are not critical, but which may prevent attainment of best practice and/or operational efficiency.