APPENDIX D1

Liverpool City Council

INTERNAL AUDIT

MFRS - INFORMATION SECURITY

FINAL REPORT

STATUS

Whilst this audit report is directed primarily to the recipients named in the report, audit reports are subject to the provisions of the Freedom of Information Act and, as such, may be required to be made publicly available upon request.

Before responding to any request to make this report publicly available, or otherwise making it publicly available, you should consult the Lead Audit Manager named in the report.

Similarly, this audit report, or extracts from it, should not be included in, or appended to, any committee report, nor should it be quoted as a background paper to any committee report without firstly consulting the Lead Audit Manager.

SUBJECT:	MFRS - Information Security
AUDIT MANAGER:	Melanie Dexter
AUDITOR:	Sam Challinor
DATE:	17/01/12
DISTRIBUTION:	Deb Appleton, Ed Franklin, Bernie Kenny

AUDIT OPINION *

The Audit Opinion has two elements. It is assessed in terms of the level of assurance in respect of the area under review and also the corporate risk impact on the council as a whole. Both are determined by the scope and results of our work.

Level of Assurance:	Significant
Corporate Impact:	Low

Heads of Services should consider whether they should refer to this assessment in their annual assurance statement on internal controls together with any actions agreed and / or taken to improve the system.

RECOMMENDATIONS SUMMARY

Priority	Category	Number in this report
★★★	Essential/Strategic	0
★★	High	2
★	Medium	1

For an explanation of audit opinion, corporate risk and recommendation gradings please see the Appendix to this report. N.B. recommendations will be followed up.

EXECUTIVE SUMMARY

An audit of the Authority's Information Security arrangements has been completed as part of the agreed 2011/12 plan of audit work for the Merseyside Fire and Rescue Service (MF&RS).

This audit review aimed to establish whether the Authority's information security policies and procedures were in line with best practice, appropriate to the needs of the organisation and adequately mitigate key risks associated with the storage and processing of information.

The Authority has put in place a robust set of procedures to protect the information it both holds and produces. These practices are largely supported by a comprehensive set of policies and guidance documents although there were instances where although an appropriate action was taking place, it was not specifically detailed in a policy or procedure note as a requirement.

There are a number of areas identified from the review that could be improved upon; however given the broad nature of this review the number of weaknesses identified were proportionately small.

The detailed findings and recommendations in this report, detailed in the table below, have been made to assist management and members in strengthening the Authority's governance arrangements.

Findings and Recommendations

No	Findings	Implications	Recommendation	Priority	Response & by Whom	Implementation Date
1	The Authority does not have a policy relating to the use of cryptographic controls.	Cryptographic controls may not be used for sensitive/critical information or may be used unnecessarily on low value/non sensitive information.	A policy should be produced, or an existing policy should be adapted, to clearly set out when and how cryptographic controls should be used.	★★	This is already an area under discussion at the Information Security Forum (ISF). a) Encrypted Memory sticks have already been covered and the SIRO will produce the Service Instruction to underpin the Information Security Policy. b) Toughbooks on fire Appliances are protected by Truecrypt Hard Disk encryption software. The ISF will need to discuss and agree if this needs to be rolled out to all Laptops or should the Service wait for the rollout of Windows7 that includes similar security measures. Ed Franklin	30/04/12

Priority	★★★	Essential/Strategic	★★	High	★	Medium

No	Findings	Implications	Recommendation	Priority	Response & by Whom	Implementation Date
2	A policy is not currently in place which stipulates that all MFRS assets in possession of employees, contractors and third parties must be returned upon termination of their contract.	Assets containing sensitive or valuable information may not be returned.	A policy should be produced, or an existing policy should be adapted, to ensure that all MFRS assets are returned to the relevant officer by employees, contractors and third parties upon termination of their contract.	★★	This is referred to in the exit Questionnaire and SI and advises that property should be returned.(This is due to go to SMG and the Authority) Pay and Pensions also advise the employee that they need to return property. Suzanne Lea – People and Organisational With regard to contractors and third parties a clause will be written into future contracts-Lindsey Savage	31/05/12
3	The Authority does not have a documented clear desk/screen policy.	Sensitive information may be accessible to unauthorised users.	The Authority should implement a corporate clear desk/screen policy.	★	A section to be included in the DP Policy about a clear desk procedure. Jean Crimmins	30/04/12

Appendix

OVERALL AUDIT OPINION levels explained

This audit report contains an opinion on the overall level of assurance that can be given on the internal control environment / systems. It will be one of four levels: High, Significant, Moderate and Limited.

The report also provides an opinion on the risk impact that the findings of the audit may have corporately. This opinion will also be one of four levels: High, Medium, Low and Negligible.

The tables below provide guidance relating to how the auditor determines the opinion level. It should be noted that the details below are written as a guide, not as a set formula. The opinion level remains at the discretion of the Lead Audit Manager and may differ from the guidance below under exceptional circumstances.

LEVEL	Explanation	Guidance
High	There is a sound system of control and governance in place to achieve the system objectives, controls are being consistently applied and the relevant risks to the business unit are well managed.	No recommendations have been made, or 1 star recommendations made that cumulatively do not warrant 'significant status'.
Significant	The control environment / systems are operating effectively to ensure that the majority of relevant risks are managed. Slight improvements need to be made in order to provide high assurance that all of the objectives of the system are met.	A 2 star recommendation made, or A large number of 1 star recommendations that cumulatively could meet the criteria for a 2 star recommendation.
Moderate	Weaknesses and / or non-compliance with procedures are placing system objectives at risk.	Improvements could be made to a number of areas within the control environment so that the relevant risks are managed more effectively, or A 3-star recommendation made, or Several 2-star recommendations that cumulatively could meet the criteria for a high priority action.
Limited	There are control weaknesses and / or non-compliance with basic controls that are so significant the relevant risks are not being managed at all. The system is open to significant error or abuse.	More than one 3-star recommendation made.

CORPORATE RISK IMPACT RATING – Explanation

Corporate Risk Impact Grading	Description of Risk
High	● Total service loss for a significant period ● Fatality of employee/service user/other person ● Adverse national media coverage ● Severe stakeholder concerns ● Mass complaints ● Financial loss in excess of £1 million
Medium	● Significant service disruption ● Major disabling injury ● National media coverage ● Significant service user complaints ● Financial loss in excess of £100,000
Low	● Limited service disruption ● Adverse local media coverage ● Some service user complaints ● Stakeholder concerns ● Financial loss in excess of £10,000
Negligible	● Short term inconvenience ● Negligible injury ● Local media coverage ● Isolated service user complaints ● Financial loss less than £10,000

AUDITOR GUIDANCE ON RECOMMENDATION RATING – Explanation

Essential / Strategic (3 star)	**High (2 star)**	**Medium (1 star)**
Absence or failure of fundamental control (i.e. no recovery action on arrears, no bank reconciliation, failure to clear significant reconciling items appropriately, no Treasury Management Strategy) where there is no compensating control	A weakness in fundamental control (i.e. not carried out on time, not authorised) Absence or failure of key controls i.e. orders not authorised, no review of bank reconciliation	General weakening of the control environment
Failure or absence of a control which would probably result in a direct risk of serious injury to staff, customers or third parties	Failure or absence of a control which would possibly result in a direct risk of serious injury to staff, customers or third parties	Failure or absence of a control which would possibly result in an indirect risk of serious injury Localised failure of a control which would possibly result in a direct risk of serious injury to staff, customers or third parties
Any illegal operation Any failure to comply with regulatory requirements	Widespread non-compliance with policy	Localised non-compliance with policy
	Absence of procedure notes Absence of clear organisation policy	Procedure notes not updated
Any national reputation impact	Any local reputation impact	
		Other actions which will improve operational efficiency