ICT Security Improvements
Project Definition Document

1 Introduction

1.1 In April 2010 the Council experienced a security incident which resulted in approximately 2 days of downtime across the whole network. The incident resulted from a virus being passed from an IT contractor's laptop into the Council's systems through the Local Area Network. In the immediate aftermath of the incident, the ICT Team:

- Ensured that all laptops were fully password protected (although not encrypted)
- That all staff were made aware of issues arising with portable media devices and advised not to use USB sticks except when necessary and only after passing USB sticks to IT for checking

1.2 A lessons learned paper was produced following the incident which established that:

- The Council and ICT staff responded well to the incident
- Systems were brought back on-line as quickly as could reasonably have been expected
- The Council's business continuity arrangements worked well

However, the review also established that although the Council have made substantial improvements to protect the security of Council systems via the Wide Area Network (mainly in response to the need to meet GCS(X) requirements), there remain a number of security weaknesses on the Council's Local Area Network. Specifically, there are control weaknesses relating to:

- Policy and the organisation's wider understanding of security issues
- the use of laptops
- the use of portable media devices, such as USB sticks
- contractors access to Council systems

There are also questions that remain to be answered relating to the use of smart phones and members' access to information using Smart phones that although they do not present a significant risk from a virus perspective, nonetheless present some risk of data loss

Driver	Programme & Monitoring Level	Corporate Ambition / Priority	Delivery Date

Driver	Programme & Monitoring Level	Corporate Ambition / Priority	Delivery Date
To improve security controls within the Council's Local Area Network as referred to above	A tier 2 project monitored by the Director of Resources within the ICT Infrastructure Programme	Move Towards Excellence/ Use Resources Effectively	June 2011

2 Deliverables

2.1 The project will deliver:

- Stricter security controls, processes and policies.
- Encrypted laptops, with appropriate patch management solutions
- A solution to better control access to the Council's network from 3rd parties, such as ICT contractors
- Managed removable media solution – Restricted USB use
- Clearer protocols regarding the use of Smart Phones
- Well informed staff able to work safely and securely
- Agreed sanctions to be agreed through an updated staff disciplinary policy

3 Business Benefits

3.1 The anticipated benefits resulting from the delivery of the project are:

- Reduced risk of virus and other forms of malicious attack
- Reduced risk of data theft and data loss
- An informed and data security aware workforce

- Reduced risk of loss of reputation due to data loss

4 Outline Plan and Approach

4.1 A staged approach is necessary to take forward these proposals. Key stages and milestones are as follows:

- Review options for tightening security from a technical perspective March 2010
- Draft policies for agreement with Data Security Group and Consultation April 2010
- Consult with Council and SHL to establish impact of policies and proposed solutions May 2010
- Implement solutions and Finalise and communicate policies in line with communications plan June 2010

Where solutions have been identified which will mitigate significant risks and where business impact is assessed as low, these solutions will be implemented straightaway. An example is lap top encryption. Encrypting laptops will not inconvenience users in any significant way and will mitigate data loss risks.

5 Resources

5.1 The project has an agreed budget of £36,000 capital (KS160) split as follows:

- £25,000 expenditure
- £11,000 of ICT internal staff time

SHL have agreed to meet approximately thirty percent of these costs in line with their overall use of ICT infrastructure.

5.2 The project will incur on-going revenue costs for which an estimate cannot be provide at this time as products have not been selected. At this stage it is anticipated that revenue costs will be absorbed within ICT budgets in future years.

5.3 Outside the ICT section, the main call on resource may be from the Council's HR Team. The key elements of the HR support will relate to:

- Approval of policies (no more than 1 working day)
- Advice on designing feedback/consultation sessions with the business focused upon understanding the impact of tightening security controls (half a day)

6 Roles and Responsibilities

6.1 It is proposed that the project will be sponsored by the Head of Customer Services & Business Improvement (Henry Lewis) and managed by the ICT Services, Security & Standards Manager (Peter Wain).

6.2 The Council's Information Security Group will act as a reference group for all key decisions made throughout the project.

7 Stakeholders

7.1 Customers, Staff and Members have all been identified as key stakeholders in the project. A detailed stakeholder analysis will be undertaken in liaison with the Council's Data Security group to inform the staff and Member consultation and engagement process.

8 Outline Communication Plan

8.1 Comprehensive communication will need to take place with the Council and SHL regarding the proposals from this project. Both organisations will need to be consulted to ensure that business needs are balanced with the tighter security proposals that are to be proposed. This will be the case particularly regarding:

- lap top usage
- use of portable media devices such as USB sticks
- new security policies

New policies and procedures will then need to be widely communicated to staff and Members and arrangements made to update induction processes etc.. Communications and consultation plans will be reviewed by the Data Security Group. A detailed plan will be drafted once a stakeholder analysis has been undertaken and the project plan finalised.

9 Constraints

9.1 The table below outlines the scope of the project and any constraints which apply:

Exclusions	Assumptions	Dependencies
Other pieces of security work directly connected with maintaining the Councils GCSX connection.	Based on research undertaken, the core assumption is that a solution is deliverable within the allocated budget. That the Council and Stevenage Homes are committed to mitigating security incidents. That the policies and procedures adopted as part of this project apply to all staff of both organisations and to elected members.	This project is dependant on the approval of security policies and processes by the security group following wider consultation. The organisation and its staff acceptance of the proposed changes.

10 Risks

10.1 The table below outlines the risks which have been identified and how these will be managed.

Risk	Initial		Mitigating Actions	Residual	
	Likelihood	Impact		Likelihood	Impact

	Initial			Residual	
Project budget overspends by up to 10%	Possible	Medium	Cover overspend on this project by using under spend within other ICT Business Improvement projects.	Not likely	None
New policies and processes unpopular	Likely	Medium	An effective communication plan applied	Possible	Minor
The Council suffer data loss	Likely	High	Apply management and audit capability of removable media. User education	Possible	High
The Councils network suffers another virus outbreak	Possible	High	Despite mitigating the risk no network is 100% secure User education	Possible	High

11 Change Management

11.1 Slippage greater than a month or of more than ten percent on the project budget will need to be agreed with the project sponsor and communicated to the Data Security Group.

12 Programme Monitoring Information

12.1 The table below provides the programme monitoring information.

Resource	Cross Cutting Resource	External Threat	Complexity	Readiness	Deferral
Medium	Medium	Low	Medium	Medium	Yes *

Cross cutting resource is identified as medium. There will be little requirement for other parts of the organisation to undertake work with the exception of HR who will need to support the development of policy. Given that HR have a very heavy workload already, this represents some risk to project implementation. The rest of the organisation will need to engage with the security solutions that are proposed. A programme of consultation and communication will be devised with the support of the Council's Training and Development Manager.

* Not undertaking the project would have the following implications:

- The risks remain high
- There is a risk that the GCSX connection will be disconnected if new security policies and processes are not adopted