Report of the Director of Policy & Resources	Decision to be taken after 29 July 2013

NORTH LINCOLNSHIRE COUNCIL

POLICY AND RESOURCES CABINET MEMBER

LAPTOP PC HARD DISK ENCRYPTION

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 The report outlines a proposal for IT Services to undertake an extensive process of hard disk encryption of all council laptop/notebook devices in order to improve security and data protection.

1.2 Key points are as follows:

- the laptop asset base has increased to c. 1,100 devices
- 410 devices are remotely used and therefore have hard disk encryption facilities installed.
- It is proposed to encrypt all laptops/notebooks for the reasons stated in the main body of the report

2. BACKGROUND INFORMATION

2.1 On 1 September 2009 the council joined the Government Connect Secure Extranet (GCSX). The GCSX network provides a secure infrastructure for councils and other public bodies to share and transfer sensitive information.

2.2 In order to join GCSX we needed to demonstrate compliance to a list of technical controls, known collectively as a code of connection (CoCo).

2.3 One of the controls stated that all laptop PCs used remotely must have the remote working solution installed, including hard disk encryption.

2.4 Technical advisors from GCSX developed a list of products to assist councils to meet numerous elements of the CoCo. This product list included several encryption tools. IT Services piloted the Becrypt Disk Protect solution and implemented the facility.

2.5 Over recent years the laptop PC estate has risen to c. 1,100 devices. Of these 410 were identified as remotely used devices and therefore have the hard disk encryption facilities installed.

2.6 Since 2009 we have successfully retained GCSx connectivity by demonstrating compliance to the GCSx CoCo. This is an annual task and will be next reviewed in August 2013.

2.7 The risks surrounding non-encrypted devices have been raised and discussed at the IT and Information Security Forum and feature in the information governance improvement plan. To assist in mitigating the associated risks, we have previously developed and distributed policies to highlight the responsibilities for securing data and educate data owners accordingly. A recent internal audit of this area resulted in an ‘adequate assurance’ classification.

2.8 Several high profile cases have again further highlighted the risks involved in not encrypting all laptop devices. The Information Commissioners Office (ICO) fined Glasgow Council £150k for the loss of two laptops. Both laptops were stolen from a council building where there were security failings. These were not seen as remote laptops and highlight the risk of not encrypting laptops not intended to be taken off site.

2.9 This case alone has indicated the obvious need to review our technical standards and procedures in order to avoid a similar scenario at North Lincolnshire Council.

2.10 This proposal excludes tablet devices. Tablet devices that are used by elected members (Apple iPads) use Enterprise Grade security. A mobile device management solution (Meraki) is in place for tablet devices to ensure they are managed accordingly. Meraki is a remote support tool that enables IT Services to assist tablet device users in a similar manner as a Microsoft Windows PC/Laptop.

3. OPTIONS FOR CONSIDERATION

3.1 Option One: Encrypt all NLC laptops using Becrypt Disk Protect.

3.2 Option Two: Encrypt devices for only remote workers and accept the risk with the remaining devices.

4. ANALYSIS OF OPTIONS

4.1 Option One: Encrypt all NLC laptops using Becrypt Disk Protect.

Advantages

- This would significantly reduce the risk of data breaches and improve overall security of council information.
- Full compliance with the 1998 Data Protection Act and IS027001 Security standard.
- The council could safely extend flexible working solutions
- Increase the awareness of data security across the council
- Familiarity and satisfaction with existing product
- Reduce alternative methods of encryption (USB Sticks)
- Positive steps to achieve GCSX compliance in August 2013
- Maintain the council’s reputation as a responsible data controller

Disadvantages

- Increased licensing costs. Initial product purchase and ongoing maintenance.
- Demands on IT technical resources for the period of the programme

4.2 Option Two: Encrypt devices for only remote workers and accept the risk with the remaining devices.

Advantages

- No additional licensing costs incurred

Disadvantages

- No reduction in the risk to the council
- Continue to rely on policies and procedures for council officers to follow for keeping data secure
- Does not assist with the flexible working arrangements
- Action could still be taken against us if laptops are stolen from council buildings, particularly if it can be determined that we have not taken sufficient care to prevent the loss.
- Increased use of USB sticks.

5. RESOURCE IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

Following a proof of concept, Becrypt is still the preferred technical solution for hard disk encryption. Becrypt is GCSX compliant and comparable in terms of cost.

By further extending the Becrypt tool we retain a single standard solution for hard disk encryption.

5.1 Financial implications:

Additional costs associated with Option 1 are detailed below:

- £27k one-off costs to procure the additional Becrypt Licences to cover the remaining laptop PC estate.

- There is an increase of £8k annual maintenance to cover the additional Becrypt licences. The new annual maintenance cost will be £11.5k.

Existing centralised IT budgets will be utilised to cover the additional license costs.

The additional encryption of laptop devices will be resource intensive and will take place over a planned prioritised period to avoid user disruption where ever possible. New devices and faulty laptops being maintained will have the product automatically installed before being returned.

ICO imposed fines and penalties for data breaches resulting from data protection failings can be in excess of £100,000

6. OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)

6.1 An Integrated Impact Assessment has been undertaken and indicated no adverse impacts arising from this report.

7. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

7.1 Becrypt Disk protect is a recognised disk encryption tool and is suggested by GCSX technical advisers as an appropriate security solution. Becrypt also complies with the latest version of CoCo (V4.1)

7.2 The Information Security Forum supports the approach to encrypt the entire council laptop estate and amend existing technical standards.

7.3 The Information, Improvement and Value for Money Group have recently requested that all new laptops are encrypted before issue. Encrypting all devices will exceed this request.

7.4 MASS Ltd (NLC IT Partner and security specialists) acknowledges the importance of encrypting all laptops and use the Becrypt product throughout the company.

8. RECOMMENDATIONS

8.1 That the proposal to commence new laptop/notebook PC encryption processes across the entire estate is approved.

8.2 That relevant IT technical security standards, policies and procedures are revised accordingly.

DIRECTOR OF POLICY AND RESOURCES

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB
Author: Carl Render/Martin Oglesby
Date: 4 July 2013

Background Papers used in the preparation of this report:
IT Technical Standards Policies