Agenda Item No 8(b)

North East Derbyshire District Council

Cabinet

11 July 2019

Payment Cards Industry – Data Security Standards (PCI-DSS) Compliance

Report of Councillor M Thacker MBE, Leader of the Council and Portfolio Holder for Overall Strategic Leadership

This report is public

Purpose of the Report

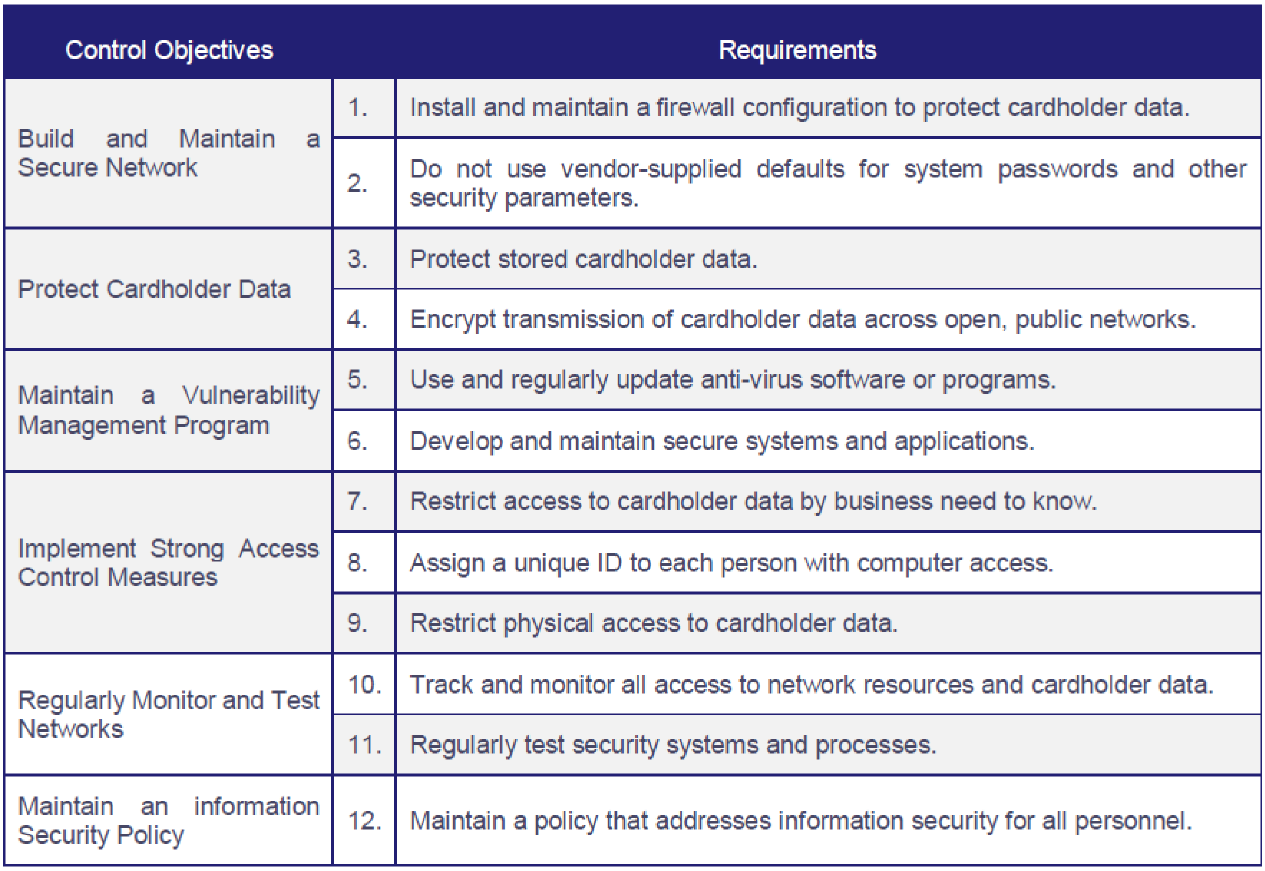
- To raise Cabinet awareness of potential cost and service implications in progressing towards Payment Cards Industry Data Security Standards (PCI-DSS) compliance.
- To recommend and seek approval for measures to facilitate progress towards compliance with the PCI-DSS.

1 Report Details

Background

1.1 The PCI Data Security Standard was originally formed by Visa and MasterCard to bring together their individual compliancy programs. Three other payment brands, American Express, Discover and JCB then joined up which lead to the PCI SSC (Payment Card Industry Security Standards Council) being formed as an independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis.

1.2 The PCI DSS covers the security of all entities that store, process and/or transmit cardholder data including; merchants, processors, acquirers, issuers and service providers as well as all other entities that store, process or transmit cardholder data. The PCI DSS is intended to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. This is built upon 12 requirements as shown in the table below; each one consisting of over 240 individual requirements (v3.2).



Control Objectives		Requirements
Build and Maintain a Secure Network	1.	Install and maintain a firewall configuration to protect cardholder data.
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3.	Protect stored cardholder data.
	4.	Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5.	Use and regularly update anti-virus software or programs.
	6.	Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know.
	8.	Assign a unique ID to each person with computer access.
	9.	Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data.
	11.	Regularly test security systems and processes.
Maintain an information Security Policy	12.	Maintain a policy that addresses information security for all personnel.

1.3 A breach of compliance involving the loss of card holder data can result in:

- ○ Significant financial penalties ranging from £1000’s to £100,000’s, enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.
- ○ In addition, related data breaches enforced by GDPR legislation
- ○ Damage to organisations reputation
- ○ Loss of customer trust

1.4 In order to reduce the scope of PCI and therefore our exposure to risk, the Council should work towards ensuring all risks associated with card payments <u>are reduced as far as is practical.</u>

1.5 A risk management approach must be taken, key elements are:

- ○ Identify all known risks and record them on a risk register
- ○ Develop a risk management program to determine the risk and identify solutions to reduce risk
- ○ Implement / work towards solutions to mitigate the risk
- ○ Continue to monitor and review

The Council operates three different payment channels; e-commerce, card-present and card-not-present. Approximate transactions over a 12 months period break down as follows:

- Telephone transactions is approx. 25,000 per year,
- E-Commerce transactions is approx. 100,000 per year,
- Pin Entry Device transactions is approx. 40,000 per year.

With the total number of transactions being approx. 165,000 per year, the Council is classed as a level 3 merchant which means a self-assessment questionnaire is completed to certify compliance.

1.6 A PCI Working Group (Inc. Rykneld Homes) was convened to fully consider the implications to the Council. To date, this group has:

- Commissioned Sec-1 Ltd Security Testing to undertake a gap analysis to identify the key areas to address.
- Received presentations from payment providers to develop understanding possible solutions for card not present payments
- Undertook corporate assessment during 2018 to identifying all non-compliance areas
- Site visits have been undertaken with other Councils to establish how they are addressing compliance.

1.7 At this point in the journey towards compliance there are two key areas that require addressing by the Council:

- Payment Kiosk at Mill Lane
- Risks inherent within the current cardholder not present payment processes

Payment Kiosk at Mill Lane

1.8 As of 1st January 2020, regulations are changing in relation to cardholder present electronic payments. All point of sale (POS) terminals must offer contactless functionality. Therefore the existing payment machine is non-compliant.

1.9 In addition, the current supplier, Banking Automation, will no longer support the payment machine beyond 31st December. By continuing to take card payments through the payment machine after this date the authority would be at risk of non-compliance. Also, due to being unsupported, the machine will not be updated to receive the new £20 in 2020.

Forecast cost in the region of £15,000 for a compliant payment machine.
The usage of the Mill Lane kiosk can be seen in the table below:

Payment Type Description	Financial Year 2016 / 2017		Financial Year 2017 / 2018		Financial year 2018 / 2019	
	No. of Transactions	Value of Transactions	No. of Transactions	Value of Transactions	No. of Transactions	Value of Transactions
Cash	1365	£142,910	1174	£143,405	980	£120,215
Cheques	5991	£3,575,622	5459	£2,271,992	3851	£1,695,337
Credit Card	79	£12,394	51	£13,553	76	£24,751
Debit Card	584	£85,488	585	£93,284	548	£108,159

Total	**8019**	**£3,816,416**	**7269**	**£2,522,235**	**5455**	**£1,948,464**
Reduction Figures from Previous Years	N/A	N/A	750	1,294,180 (34%)	1814	£573,771 (22%)

1.10 To address this issue it is recommended that Cabinet considers two options:

Option 1 - Replace payment kiosk at Mill Lane
Cost of £11k for the new kiosk and upgrade of Smart Gateway (Capita Integration) to version 10 to support Chip & Pin.

Option 2 – Remove the kiosk at Mill Lane

- Minimal cash taken at Mill Lane (£10k per month)
- Aligns with strategic transformation aims
- Cost saving on cash handling of £6,000

Where a similar facility was removed from Eckington Pool, following the refurbishment, closure commenced from 28th October 2016. The Council received 1 formal complaint by way of a petition and the local community have found alternative methods of payment such as:

- 24 hours a day via the website www.ne-derbyshire.gov.uk using a debit card
- 24 hours a day automated payment line (Council Tax only)
- Area Housing Offices (Killamarsh, Dronfield, Clay Cross, North Wingfield)
- At any Post Office or PayPoint outlet by cash or debit card using your Council Tax bill
- Card payments taken during opening times via a secure payment line by the Customer Service Advisors
- Standing Order, you arrange with your bank, payment date of your choice

Customer Not Present payments

1.11 Our current telephone payments process for Customer Not Present card payments is currently not PCI-DSS compliant. Currently an officer taking payments must enter the card details on behalf of the customer into our payments solution. To mitigate risks inherent in this process, it is necessary to remove the exposure of the officer from the customer's card details.

1.12 To address the compliance issue two options are proposed:

1. Capita, our payments solutions provider, have an 'off the shelf' solution called 'Call Secure', the revised process would be:

    a) Officer captures customer details up to the stage of the card detail entry, at which point:
    b) To help safeguard the customers card the officer transfers to an automated service to take their card details
    c) Customer enters card details (card number, start date etc.) using a telephone keypad - fund and account details are pre-populated
    d) Officer sees ***** as the payment progresses. When the payment processed securely a reference number is issued.

The cost of this solution is an initial £16.5k investment, plus £12k per annum licence fee.

2. An extension of the current Automated Telephone Payments (ATP) solution. Currently, the Council utilise an ATP to take telephone payments for Council Tax. This solution would involve engaging Capita to implement additional payment fund types and some work from ICT, Customer Service and Finance to implement. It is understood that this would provide a similar outcome as the Capita Call Secure solution (as above) but at less cost. The revised process would be the similar to that outlined above but there would be no visibility of the masked entry of card details by the customer. The advisor will then need to log into the reporting system to check the payment has successfully processed and obtain the reference number. This solution needs further testing from both a technical and customer service perspective.

The cost of this solution is currently unknown and testing is underway to ensure the solution is deliverable. However, it is anticipated that should the solution work, it will be more cost effective than the Capita Call Secure Solution.

1.12 It should be noted that Rykneld Homes currently have non-compliant payment kiosks in the Area Housing Offices & One Stop Shops. RHL are working with the kiosk provided and are confident existing kiosks can become PCI compliant with minor upgrades from the supplier.

2 Conclusions and Reasons for Recommendation

2.1 The report aims to raise Cabinet's awareness of an emerging compliance issue that could result in significant additional cost to the Council. Officers will continue to develop the solutions and will present a final proposal in a further report close to the end of the calendar year.

2.2 Whilst this work progresses, it is recommended that Officers begin to progress Option 2 outlined in paragraph 1.10 by actively communicating, providing support to utilise alternative payment options and drive down demand for the Kiosk at Mill Lane.

2.3 In addition, resource will be committed to progress with the ATP solution for Card Holder not Present payments as described in section 1.11, with the Capita Call Secure Solution as 'back-up' should the solution not deliver as anticipated.

2.4 The recommendations seek to provide a practical and economical solution to ensure PCI DSS compliance, whilst maintaining or enhancing the customer experience and trust in the Council when it comes to personal data.

3 Consultation and Equality Impact

3.1 Consultation has initially been undertaken with the relevant departments such as ICT, Finance, Customer Services and Rykneld Homes

3.2 Procurement and Legal will be engaged prior to any procurement exercise.

4 Alternative Options and Reasons for Rejection

4.1 At this time the alternative options whilst not being actively pursued have not been ruled out. A further report will be provided to present the implication and progress of driving down demand for the kiosk and the feasibility of the ATP solution.

5 Implications

5.1 Finance and Risk Implications

5.1.1 No funding is required at this stage to support the implementation of the recommendations.

5.1.2 There is a risk that whilst driving down demand for the Mill Lane Kiosk, we disappoint customers as they feel we are 'withdrawing a service'. This may result in a number of complaints. However, this report aims to mitigate risk by managing customer expectations and communicating effectively that the Kiosk function will not be available from 1st January 2020 and offer support in accessing alternative payment methods.

5.2 Legal Implications including Data Protection

5.2.1 In order to reduce the scope of PCI, organisations should work towards ensuring all risks associated with card payments are reduced as far as is practical.

This reports demonstrates that we are working towards practical solutions however, a breach could result in:

- Significant financial penalties ranging from £1000's to £100,000's, enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.
- In addition, related data breaches enforced by GDPR legislation
- Damage to organisations reputation
- Loss of customer trust

5.3 Human Resources Implications

5.3.1 There are no Human Resource implications in relation to these proposals other than the effective use of existing staffing resource.

6 Recommendations

6.1 That Cabinet note the content of the report and acknowledge potential cost implication outlined within the report.

6.2 That Cabinet support actively driving down demand for the Kiosk in the Contact Centre through effective communication and support to customers.

7 Decision Information

Is the decision a Key Decision? A Key Decision is an executive decision which has a significant impact on two or more District wards or which results in income or expenditure to the Council above the following thresholds: *BDC: Revenue - £75,000* □ *Capital - £150,000* □ *NEDDC: Revenue - £100,000* □ *Capital - £250,000* □ ☑ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
Has the relevant Portfolio Holder been informed	Yes
District Wards Affected	All
Links to Corporate Plan priorities or Policy Framework	All

8 Document Information

Appendix No	**Title**

Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet (NEDDC) or Executive (BDC) you must provide copies of the background papers)	
Sec-1 Ltd Report: Cardholder Data Environment Mapping – Oct 18	
Report Author	**Contact Number**
Matt Broughton Head of Service Partnerships and Transformation	2210