Document 2.3B

CARDHOLDER DATA SECURITY POLICY

Adopted 27 March 2017
Review by March 2018

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential card payment data and must be brought to the attention of all employees. All employees must read this document in its entirety and sign the form confirming they have fully read and understand this policy. This document will be reviewed and updated by Council on an annual basis or when relevant to comply with the standards required by the Payment Card Industry's Data Security Standard (PCI-DSS) and distribute it to all employees and contracts as applicable.

2. Information Security Policy

Hertford Town Council handles sensitive cardholder information daily. Sensitive information must have adequate safeguards in place to protect the data, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Hertford Town Council commits to respecting the privacy of all its customers and to protecting any cardholder data from outside parties. To this end, the Council is committed to maintaining a secure environment in which to process cardholder information in order to meet these promises.

Employees handling sensitive cardholder data should ensure:

- Cardholder information is handled and protected in a sensitive manner.
- Personal information is not disclosed unless authorised.
- Passwords and accounts are kept securely.
- Approval is requested from Council prior to establishing any new cardholder software or hardware, third party connections, etc.
- Desks are left clear of sensitive cardholder data and any files or equipment containing such information is locked away, when unattended.
- Information security incidents are reported, without delay, to the RFO or Town Clerk and such incidents are swiftly dealt with and reported.
- All staff have a responsibility for ensuring Council's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager. Hertford Town Council will not receive or retain any card details on any computer or email.
- Information from cardholders is only be held in paper format and card details are protected and all files will be locked away when not in use.

3. Acceptable Use Policy

The Council's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Hertford Town Council's established culture of openness, trust and integrity.

The Council is committed to protecting the employees and councillors from illegal or damaging actions by individuals, either knowingly or unknowingly. Hertford Town Council will maintain an approved list of card payment technologies and devices and personnel with access to such devices as detailed in Appendix B

Employees should take all necessary steps to prevent unauthorised access to confidential data which includes card holder data.
Keep access to the cardholder equipment secure and do not share passwords. Authorised users are responsible for the security of these items so they cannot be tampered, altered or accessed for personal use.

Hertford Town Council will not receive or retain any cardholder information in any electronic or computer format including emails.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be considered as acceptable for non-compliance.

5. Protect Stored Data

All sensitive cardholder data stored and handled by Hertford Town Council and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by Hertford Town Council for business reasons must be discarded in a secure and irrecoverable manner.

6. Information Classification

It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.

- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.

- The Personal Identification Number (PIN) or the encrypted PIN Block under any circumstance

Information Classification

Card data and media containing such data must always be labelled to indicate sensitivity level:

Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Hertford Town Council if disclosed or modified. **Confidential data includes cardholder data**.

Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure;

Public data is information that may be freely disseminated.

7. Access to the sensitive cardholder data:

All access to sensitive cardholder information should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

Any display of the card number should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.

Access to sensitive cardholder information, personal information and business data is restricted to authorised employees that have a legitimate need to view such information.

No other employees should have access to this confidential data unless they have a genuine business need and have authorisation from The Town Clerk or RFO.

If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.

Hertford Town Council will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the cardholder data that the Service Provider possesses.

The company will have a process in place to monitor the Payment Card Industry Data Security Standard (PCI DSS) compliance status of the Service provider by the RFO and also through the internal audit and council's governance inspection.

Hertford Town Council will ensure that an established process including proper due diligence is in place before engaging with a third party service provider. However, the Council does not currently, and does not plan to employ such a provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data, including:

Media in any digital or physical medium (eg printed or handwritten paper, received faxes, USBs, back-up tapes, computer hard drive, etc).

Media containing sensitive cardholder information, must be handled and distributed in a secure manner by trusted individuals.

9. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

Card holder data must never be sent over the internet via email, instant chat or any other end user technologies.

If there is a business justification to send cardholder data via email then it should be done after authorisation and by using a strong encryption mechanism.

The transportation of media containing sensitive cardholder data to another location must be authorised by The RFO, Town Clerk or council and must be logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10. Disposal of Stored Data

All data must be securely disposed of when no longer required by Hertford Town Council, regardless of the media or application type on which it is stored.

All hard copies containing the full card details must be manually destroyed when no longer required for valid and justified business reasons.
Hertford Town Council has procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into the Council's practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees.

Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day practice.

Distribute this security policy document to all employees to read. It is required that all employees with contact to card details, confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)

All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI DSS).

12. Security Management / Incident Response Plan

Employees of the Council will be expected to report any security related issues to the RFO or Town Clerk who are responsible for the effective communication of financial security policies and procedures to employees. In addition to this, the RFO or Town Clerk will monitor and enforce the card related security policies outlined in this document and oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Incident Response Plan

In the event of a suspected security breach, alert the RFO or Town Clerk immediately.

The RFO or Town Clerk will carry out an initial investigation of the suspected security breach.

Upon confirmation that a security breach has occurred, the RFO or Town Clerk will inform all relevant parties that may be affected by the compromise.

If the data security compromise involves credit card account numbers, the following procedure will be implemented:

Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.

Alert all affected parties and authorities such as the Merchant Bank, Visa Fraud Control, and the police if necessary.

13. Tampering of Equipment

Devices are inspected monthly for tampering and the dates of inspection will be recorded. Types of tampering can include additions of card skimmer hardware or a swapping of devices. Serial numbers of devices are verified.

Appendix A

Agreement to Comply Form – Agreement to Comply with Cardholder Data Security Policy

_____

Employee Name (printed)

_____

I agree to take all reasonable precautions to ensure that Council's internal information, or information that has been entrusted to the Council by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Council, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the RFO or Town Clerk who are the designated security officers.

I have access to a copy of the Cardholder Data Security Policy, I have read and understand the policy, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policy and other requirements found in the Council's card security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to report promptly all violations or suspected violations of information security policies to the designated security officer.

_____

Employee Signature

_____

Date

Appendix B

Card processing equipment in use

Asset/Device Name	Serial Number	Owner/Approved User	Location
IGENICO IWL250			Castle Reception
IGENICO ICT 250			Town & Tourist Information Centre

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date