Information Security Policy

1.Introduction

Gemporia recognises that payment card information is a valuable asset. Managing supporting systems and the information they contain is vital to maintain Gemporia’s reputation and the ability to continue trading successfully.

Gemporia considers the security of its cardholder data environment (CDE) and cardholder data to be a crucial element of its business and, to this end, has created a well-defined set of policies, standards and procedures to support secure operations

The aim of this policy document and its Appendices is to set out the principles that guide how Gemporia will maintain the confidentiality, integrity and availability of cardholder data.

2.Scope

This policy applies to the people, processes and technology that store, process or transmits cardholder data or sensitive authentication data, including any connected system components.

The IT Director maintains the list of systems components that comprise the cardholder data environment (CDE).

Where a policy statement cannot be met by the technical controls available on a system, this shall be indicated in the relevant System Configuration Document, and compensating procedural controls implemented and documented to ensure that this policy is fully complied with. Where there is a legal or legitimate business reason why a policy statement or PCI DSS requirement cannot be met this shall be documented.

3.Policy Statement

3.1.Overall statement

1. This information security policy shall be established, published, maintained and disseminated to all relevant personnel (including system users, employees, vendors, contractors and business partners) (12.1);
2. This information security policy shall include an annual process that identifies threats together with vulnerabilities and results in a formal risk assessment (12.1.2);
3. This information security policy and its appendices will be reviewed at least once a year and updated when the cardholder data environment changes (12.1.3).

4.Information Security Roles at Gemporia

Responsibility	Role responsible
Overall responsibility for cardholder data security and owner of this policy	IT Director
Overseeing Information Security	IT Director
Creating and distributing security policies and procedures	IT Director
Monitoring and analysing security alerts	IT Director
Distributing information to appropriate information security and management personnel	IT Director
Creating and distributing security incident response and escalation procedures	IT Director
Owner of cardholder data	IT Director
Administering user account and authentication management	IT Director
Protecting card data proactively	All Staff
Following up and resolving instances of non-compliance with Gemporia security requirements	IT Director
Managing security awareness programme	IT Director
Managing the Firewall	Network Manager
Managing other network devices	Network Manager
Managing the IDS	Network Manager
System development	IT Director
Physical access security	Operations Directory
Carrying out background checks on prospective members of staff	HR Manager
Authorising changes to systems and processes within the cardholder data environment	IT Director
Conducting daily reviews of logs generated by systems within the CDE	IT Director

4.1 Standard and procedures

This policy will be supported by documented standards and operational procedures. These will be kept up to date to reflect changes to the CDE and newly identified vulnerabilities and best practices, and shall be reviewed at least annually.

4.2 Network Security

1. Network perimeter and internal security devices (e.g. firewalls) shall be installed and their configurations appropriately maintained to protect cardholder data;
2. Vendor supplied defaults shall be changed for all systems (e.g. passwords and other security parameters).
3. All remote access to the CDE shall be encrypted over a suitable channel, e.g. VPN, and must incorporate Two Factor Authentication in order to gain access

4.3 Protection of Cardholder Data

1. Stored cardholder data shall be protected by being rendered unreadable in storage;
2. Transmission of cardholder data across open, public networks shall be encrypted.
3. Unencrypted PAN details shall never be transmitted over unsecure communication lines

4. PANs will always be masked to 6 first and 4 last digits at most
5. If processes require data or media to be removed from the CDE then appropriate controls and policies must be constructed and adhered to

4.4 Vulnerability Management Programme

1. Anti-malware software (e.g. anti-virus and anti-spyware) shall be used and regularly updated in all system components that are exposed to malware attacks;
2. Systems and applications development and maintenance shall be performed in a timely and secure manner (e.g. patching kept up to date and vulnerability scans performed);
3. There shall be a process to identify new security vulnerabilities and to address these in accordance with a risk ranking.
4. All system components and software shall have the latest vendor-supplied security patches installed. The maximum period of time to install any given critical security patch on all relevant production systems will be 30 days from its release date.
5. Windows updates will be installed based on Microsoft’s recommendations and security guidance. Other hardware should have relevant security bulletins monitored.
6. Change control procedures shall be followed when applying any system and software configuration changes in accordance with the Change Control policy and procedures

4.5 Change Control and Configuration Management

1. Any changes to the CDE shall comply with a documented change control process;
2. Changes made in the CDE shall be approved by the relevant management personnel;
3. The current configuration of all the systems (hardware and software) included in the CDE shall be documented and kept up to date;
4. All system components shall comply with defined configuration standards.
5. All new vendor hardware must have default passwords, accounts and connections changed or disabled before installing the system on the network. This includes, but not limited to, default password, default username (where possible), SNMP strings.

4.6 Access Control

1. Logical and physical access to cardholder data and/or the CDE shall be restricted to all users and systems on a ‘need to know’ basis by using appropriate authentication and authorisation mechanisms;
2. The accountability of all users within the CDE shall be enforced on an individual basis;
3. Physical access to cardholder data and the CDE shall be appropriately restricted.
4. Users will be given the least privileges necessary to perform their role effectively

4.7 Monitoring and Testing Security Measures

1. Access to network resources and cardholder data shall be monitored through logging mechanisms and the logs subject to daily review;
2. All security systems and processes shall be tested at least quarterly and also whenever a major change is made in the CDE (software or hardware).
3. All security events are to be logged and reviewed at least daily, exceptions and anomalies are

recorded
4. All logs of security components for security components which transmit CHD
5. All logging must be backed up and immediately available for 3 months, available for up to 1 year
6. Intrusion detection events will be logged
7. All logging systems and critical equipment in the CDE will have their clocks synchronized to external sources such as NTP
8. All logging is to be periodically reviewed against Gemporia's risk management strategy
9. Exceptions and anomalies are recorded and prioritised accordingly in the Event log

4.8 Comprehensive Documentation

1. All security policies, daily operational procedures and standards shall be documented and kept up to date;
2. Policies and supporting documentation shall be reviewed annually;
3. All documentation shall be distributed on a 'need to know' basis, to all personnel, including employees, contractors and third parties with access to the CDE.

4.9 Critical Technologies

1. All use of technologies shall be explicitly authorised, and shall only be authorised where necessary. This includes the following within the CDE: remote access, wireless , email systems and internet access
2. Use of these technologies shall be only for their intended purpose(s)

4.10 Encryption

1. Strong encryption will be applied if the storing of card data is essential and justifiable

Note: TLS 1.0 migration strategy applies here

Sanctions

Instances of non-compliance with this policy shall be identified, documented and escalated according to the Incident Response Policy. The Issue Owner shall implement remedial measures as quickly as possible. Deliberate non-compliance by individuals, whether they are system administrators or other users, shall be treated as a disciplinary offence.

Revision History

Date	Description	Who
12/10/2014	Original Document	Andrew Smith
13/10/2015	Added Critical Technologies policy (12.3) Added 4.4.5 to cover point 2.5	Andrew Smith
20/11/2015	Added 4.6.4	Andrew Smith

Date	Description	Who
31/11/2015	Updated 4.5.5 to explicitly address “accounts” and made clear this had to happen before installation Added 4.3.3 and 4.3.4 Added 4.10	Andrew Smith
01/12/2015	Added 4.2.3, 4.3.5, 4.7.9	Andrew Smith
23/02/2016	Review, no change	Andrew Smith
24/05/2016	Review, no change	Andrew Smith
24/08/2016	Change TGGC to Gemporia	Andrew Smith