Information Security Policy

March 5, 2020

Galls, LLC

Revision History

Date	Version	Comments
03/05/2020	0.1	Initial Draft
05/07/2020	0.2	Added data retention schedule

Contents

Document Overview

Purpose

This policy document establishes specific requirements for the management and control of critical business information assets of Galls. They set forth management expectation for the protection of critical information assets processed and stored on all platforms, including stand-alone and networked systems, telecommunications systems, remote access, client-server environments, and gateways to non-Galls managed systems.

The controlled access to, and use of, information must conform to generally accepted practices, policies, and regulations. Adherence to these polices will ensure the integrity and validity of Galls information.

Scope

All employees are responsible to know and adhere to the policies herein.

These are enterprise-wide policies. No subsidiary, affiliate or location may modify, add, delete or substitute their own policies. In some cases, due to specific business regulations and /or state or country regulations, additions or changes may be necessary to some of these policies. Any addition, deletion or change to these policies must be submitted to the Chief Security Officer for review, with the reasons for the request. If approved, an addendum will be made to the policies. This will allow for the maintenance of a single set of policies rather than having multiple subsidiary-specific versions. The policies are to be delivered to new employees upon hire and completion of orientation training. Ongoing dissemination of the policies to all relevant users, employees, and contractors will be facilitated through accessibility to electronic copies, made available on an internal network share or web-based application.

Definitions

Throughout the document several different words are used to convey the requirements of these policies. The common understanding of these words is given below:

- Must, will, shall – these terms denote a mandatory requirement that must be adhered to by all. The only allowable deviation is through a formal exception waiver.
- Should – this term denotes a highly suggested, but not mandatory, recommendation.
- May, can – these terms denote non-mandatory recommendations.

Policy Statements

*The following statements are **required** policy elements for PCI-DSS v3:*

1. Network and Systems Security

1.1. Galls shall install and maintain security controls to protect against unauthorized access to internal and sensitive networks and systems.

1.2. Galls shall ensure the non-use of vendor-supplied configuration defaults (e.g. passwords, parameters, etc.) for all networks and systems.

2. Protecting Data

2.1. Galls shall ensure the protection of data through secure handling and storage to prevent unauthorized disclosure.

2.2. Galls shall ensure the protect transmission of sensitive data over untrusted communication through use of strong security controls, such as encryption, to prevent unauthorized disclosure.

3. Vulnerability Management Program

3.1. Galls shall install and maintain anti-malware measures to prevent compromise of any company system.

3.2. Galls shall ensure the secure development and maintenance of systems and applications to prevent unauthorize access to, disclosure, or modification of sensitive information.

4. Access Control

4.1. Galls shall restrict access to sensitive data in accordance with the principals of “least privileged” and “business need-to-know.”

4.2. Galls shall ensure authorization of access to networks, systems, and information through secure identification and authentication controls.

4.3. Galls shall restrict access to networks, systems, and information through physical security controls.

5. Security Monitoring and Testing

5.1. Galls shall track and monitor all access to network resources and sensitive information.

5.2. Galls shall regularly test security systems and security processes.

6. Information Security Program

6.1. Galls shall develop and maintain a security risk management program.

6.2. Galls shall develop and maintain a security awareness program.

6.3. Galls shall develop and maintain standards in support of, and as an extension to this policy, to address system- and process-specific security controls.

6.4. Galls shall ensure the screening of potential personnel prior to hire to minimize the attacks from internal resources.

6.5. Galls shall develop and maintain a third-party risk management program.

6.6. Galls shall develop and maintain a security incident response program.

Governance

Key Responsibilities

Chief Information Officer:

- Establishing management direction on behalf of the CEO and Board of Directors.
- Senior approving manager for this policy.

Chief Security Officer:

- Owner and maintainer of the Information Security Policy and program charter.
- Reporting information security metrics and key performance indicators.
- Governing and assuring the achievement of information security control objectives.
- Owner and maintainer of information security incident management.

Management:

- Adherence to the directives established by the policy herein.
- Owner and maintainer of specific information security controls.

Non-Management:

- Adherence to the directives established by the policy herein.

Enforcement

Compliance Measurement:

- The Chief Information Officer or Chief Security Officer will review this policy at least annually.
- The Chief Security Officer will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy.

Exceptions:

- Exceptions to the Information Security Policy will be maintained by the Chief Security Officer. Any exception to the policy must be approved in advance by the Chief Information Officer or Chief Security Officer. All exceptions to this policy will reviewed at least annual.

Non-Compliance:

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Key Documents / Tools / References

- Code of Conduct
- Terms and Conditions of Employment
- Data Retention Schedule (Appendix B)
- Information Security Standards

Appendix A: Galls to PCI-DSS Control Objective Mapping

Control Category	Galls Ref	Control Objective	PCI-DSS v3	Control Detail
Network and Systems Security	IS 1.1	Galls shall install and maintain security controls to protect against unauthorized access to internal and sensitive networks and systems.	R1	Install and maintain a firewall configuration to protect cardholder data
	IS 1.2	Galls shall ensure the non-use of vendor-supplied configuration defaults (e.g. passwords, parameters, etc.) for all networks and systems.	R2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protecting Data	IS 2.1	Galls shall ensure the protection of data through secure handling and storage to prevent unauthorized disclosure.	R3	Protect stored cardholder data
	IS 2.2	Galls shall ensure the protect transmission of sensitive data over untrusted communication through use of strong security controls, such as encryption, to prevent unauthorized disclosure.	R4	Encrypt transmission of cardholder data across open, public networks
Vulnerability Management Program	IS 3.1	Galls shall install and maintain anti-malware measures to prevent compromise of any company system.	R5	Protect all systems against malware and regularly update anti-virus software or programs
	IS 3.2	Galls shall ensure the secure development and maintenance of systems and applications to prevent unauthorize access to, disclosure, or modification of sensitive information.	R6	Develop and maintain secure systems and applications
Access Control	IS 4.1	Galls shall restrict access to sensitive data in accordance with the principals of “least privileged” and “business need-to-know.”	R7	Restrict access to cardholder data by business need-to-know

	IS 4.2	Galls shall ensure authorization of access to networks, systems, and information through secure identification and authentication controls.	R8	Identify and authenticate access to system components
	IS 4.3	Galls shall restrict access to networks, systems, and information through physical security controls.	R9	Restrict physical access to cardholder data
Security Monitoring and Testing	IS 5.1	Galls shall track and monitor all access to network resources and sensitive information.	R10	Track and monitor all access to network resources and cardholder data
	IS 5.2	Galls shall regularly test security systems and security processes.	R11	Regularly test security systems and processes
Information Security Program	IS 6.1	Galls shall develop and maintain a security risk management program.	R12.2	Maintain a policy that addresses information security for all personnel
	IS 6.2	Galls shall develop and maintain a security awareness program.	R12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.
	IS 6.3	Galls shall develop and maintain standards in support of, and as an extension to this policy, to address system- and process-specific security controls.	R12.3	Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.
	IS 6.4	Galls shall ensure the screening of potential personnel prior to hire to minimize the attacks from internal resources.	R12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.
	IS 6.5	Galls shall develop and maintain a third-party risk management program.	R12.8	Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data

	IS 6.6	Galls shall develop and maintain a security incident response program.	R12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.

Appendix B: Data Retention Schedule

Data Category	Retention Period
Email	3 years
All other data	7 years