The Reinalt – Thomas Corporation
20225 N. Scottsdale Rd.
Scottsdale, AZ 85255
(480) 606-6000

The Reinalt - Thomas Corporation

Information Security Policies and Procedures

Effective July 21, 2023

Revision History

Filename	Date
DTC_Security_Policy_Master_Final v2.doc	9/11/08
DTC Security Policy – Public v2.2.docx	9/11/09
DTC Security Policy - Public v2.3.docx	7/13/10
DTC Security Policy - Public v2.4.docx	12/12/11
DTC Security Policy - Public v2.5.docx	9/1/16
DTC Security Policy - Public v2.6.docx	9/1/17
DTC Security Policy - Public v2.7.docx	9/1/18
DTC Security Policy - Public v2.8.docx	9/1/19
DTC Security Policy - Public v2.9.docx	3/1/21
DTC Security Policy - Public v2.9.docx	7/1/21
DTC Security Policy – Public v3.0.docx	9/1/22
DTC Security Policy – Public v4.docx	7/1/23
DTC Security Policy – Public v4.1.docx	7/23/2023

Table of Contents

1. POLICY ROLES AND RESPONSIBILITIES

1.1 Policy Applicability

All employees, contractors, consultants, and vendors who use, maintain, or handle Company systems or information must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the Chief Information Officer (CIO).

1.2 Chief Information Officer (CIO)

The CIO is responsible for the following:

- Has overall responsibility for ensuring the integrity and security of the Company's Information.
- Delegate's development of the Information Security Policies and Procedures (Policies) to the Security Team & oversight for information security policy development to the Chief Information Security Officer (CISO).
- Delegate's implementation of Policies and Procedures to the Information Security Team, Information Security Department, and CISO.
- Approves any exceptions to Policies and Procedures.

1.3 Chief Information Security Officer (CISO)

The Chief information Security Officer is responsible for the following:

- Establishes Policies and provides oversight for Information Security policy development.
- Communicates the Policies to Business Segments and Information Technology.
- Implements the Policies by working with department managers, administrators, and users to develop security standards and procedures to help secure the Company's information systems and associated data.
- Monitors adherence to the Policies from a business process perspective.

1.4 Information Security Department

The Information Security Department is responsible for the following:

- Assists the I.T. Department in implementing Policies by working with department managers, administrators, and users to develop security standards and procedures to help secure the Company's Protected Information.
- Maintains a formal Security Awareness Program to make all employees aware of the importance of securing Protected Information.
- Ensures completion of tasks as required by the *Periodic Operational Security Procedures, Appendix N*.
- Ensures annual acknowledgement of Acceptable Use Policy.
- Performs technical security assessments on new and existing IT technologies and services including cloud and 3rd party hosted services.
- Review of Master Service Agreements and Statements of Work for appropriate security verbiage.
- Evaluate Policies from a technical perspective.
- Leads, is a member of, or provides security consultation to the organizations technical working groups or project teams.

- Reviews the Policies periodically and recommends modifications and/or additions to the CISO, as necessary.

1.5 Enterprise Security Architecture

The Enterprise Security Architect is responsible for the following:

- Partner with Business, Solution and Data Architects to gather business requirements and determine privacy, compliance, security requirements and necessary controls.
- Development of Enterprise Security Architecture strategies, roadmaps, and standards in collaboration with Enterprise Architecture.
- Research and adoption of emerging security technologies and frameworks.
- Participates in the development of Information Security policies, compliance, and risk management efforts.
- Member of the Architecture Review Board representing the Information Security Department.

1.6 Information Management & Compliance Team

The Regulatory Compliance Team is responsible for the following:

- Monitoring system components that store, process, or transmit the Company's Protected Information in relation to applicable laws and regulations.
- Monitors adherence to the Policies from a technical perspective.
- Completes tasks as assigned by the *Periodic Operational Security Procedures, Appendix N*.
- Administers the Azure Security & Compliance portal.
- Maintains awareness of existing and new risks.
- Disseminates the Company's Policies and Acceptable Use guidelines to vendors and business partners.
- Implements the Policies by working with department managers, administrators, and users to develop security standards and procedures to help secure the Company's Protected Information.

1.7 Human Resources

Due to its direct and constant relationship with existing employees and having the first and last interactions with new/terminated employees, Human Resources has a key role with regards to the Company's information security. The following items are their ongoing responsibilities:

- Publish and disseminate the Policies and Acceptable Use Policy to all relevant system users, employees, contract employees and temporary employees.
- Perform background checks on potential employees who have access to Protected Information.
- Work with the CISO and the Information Security Department on disseminating security awareness information to system users.
- Administer sanctions and disciplinary action relative to violations of Policy.
- Maintain all Acceptable Use Policy and *Employee Data Change, Appendix B* forms in employee files.
- Maintain *Encryption Key Custodianship Form, Appendix I* in employee files for those individuals authorized to access the Company's Encryption Key system.

1.8 Contract Compliance

Contract Compliance is responsible for the following:

- Provide guidance for the contract review process.
- Assist in evaluating policy from a legal perspective.
- Ensure contracts reviewed have appropriate language regarding the protection of the Company's information.
- Maintains a list of IT service providers to review compliance with documented security standards.

1.9 Users – Employees, Contractors, Consultants and Vendors

Each user of the Company's computing and information resources must realize the fundamental importance of information resources and recognize his/her responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all Company information system users:

- Understand the consequences of their actions regarding computing security practices and act accordingly.
- Maintain awareness of the contents of the information security policies. Read and sign the *Acceptable Use Policy, Appendix A*.
- Classify Protected Information that is received. Limit the distribution of this information accordingly.

2. IT CHANGE CONTROL POLICY

2.1 Policy Applicability

All proposed changes to the Company's network devices, systems, and application configurations outside of Standard Operating Procedures must follow this policy.

I.T. Department Managers or Assistant Managers will designate representatives from each of their departments to be on the Change Control Committee. Representation of the Security Team on the Change Control Committee is required.

The I.T. Support and Operations Business Unit owns the process and procedure for submitting Change Controls. Refer to ServiceNow KB0018998 for established policy.

3. INFORMATION CLASSIFICATION AND CONTROL POLICY

3.1 Policy Applicability

All employees, contractors, consultants, and vendors who use, maintain, or handle Company systems or information must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

3.2 Information Classification

3.2.1 Introduction

All information stored on the Company's computing systems must be assigned a classification level as defined by this policy. The classification levels are used to determine which users are permitted to access the information.

3.2.2 Information Categories

Protected Information – Refers to the most sensitive, regulated business information that is intended for use by the Company. Unauthorized disclosure could seriously and adversely impact the Company, its shareholders, business partners, and/or customers. Examples of Protected Information include PCI cardholder data, credit card summary reports, and encryption keys.

Primary Account Number or PAN wherever displayed whether digital or physically provided shall follow proper masking procedures. Only display of first 6 digits and last 4 is allowed unless specially authorized by the CIO. All roles that do not retain authorization to view PAN will only be allowed to masked PAN.

All allowance authorizations must be documented. A proper business justification for allowance must be documented as well as role or roles specifically granted the allowance to view PAN unmasked.

Confidential Information - Applies to less sensitive business information that is intended for use by the Company. Unauthorized disclosure could adversely impact the Company, its shareholders, business partners, and/or customers. Examples of confidential information include Human Resources and Legal information, audit reports, profit and loss statements, and passwords.

Public Information - Applies to all other information which does not clearly fit into either of the above two classifications. Unauthorized disclosure does not seriously or adversely impact the Company.

Privileged Information – Information prepared by, at the request of, or for an attorney retained or employed by the Company. All privileged information is also confidential.

All Protected Information must be subject to access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. All access to any database containing Protected Information must be authenticated. This includes access by applications, administrators, and all other users. Access controls must track all access to such information, identifying who accessed it and when it was accessed. See *Obfuscation – Data Obfuscation Matrix* on the Knowledge Center for additional information on data classification and obfuscation methods.

With role-based access control (RBAC), employees will be authorized to access information according to job role and need to know.

System Access Requests must be submitted through the ServiceNow Service Catalog to document that the appropriate approvals are received, and minimum access is granted, as requested.

3.3 Document Labeling

Documents containing Protected Information and Confidential Information, described in section 3.2.2 Information Categories, should have labels on the bottom of each page of the document stating, "Confidential Information."

If uncertain of the sensitivity of a particular piece of information, contact your manager.

3.4 User Authentication to Protected Information

3.4.1 Users

Each user's access privileges shall be authorized, according to business needs. User access authority to computer resources shall be provided only when necessary to perform tasks related to the Company's business.

The use of non-authenticated (i.e., no password) user IDs or IDs not associated with a user is prohibited. Shared or group user IDs are not permitted for user-level access.

Every user must have unique user identification (ID) and a personal undisclosed password to access the Company's computer systems. Systems and applications must authenticate using a password or token entry.

Accounts used by vendors for remote maintenance should be enabled only during the time needed.

Accounts with elevated privileges must use two-factor authentication for the purposes of system administration.

At least annually, all users must acknowledge understanding of the Policies by reading and signing the Acceptable Use Policy.

3.4.2 Systems

Each system shall have an automated or procedural access control process. At a minimum, the process must:

- Identify each user through a unique user identifier (user ID).
- Authenticate each user ID with a password.
- Require all passwords to be at least eight (8) characters in length.
- Require elevated accounts/administrative accounts to have passwords at least twelve (12) character in length.
- Require complex passwords and not use common easy to guess words.
- Require that new passwords cannot be the same as the four previously used passwords.
- Lock out accounts after six invalid logon attempts.
- Require that if an account is locked out, it will remain locked for at least 30 minutes or until an Administrator unlocks the account. If a user requests a password reset via phone, email, web, or other non-face-to-face method, the user's identity must be verified before the password is reset. The user must supply the appropriate items of identification to complete proper verification.
- Require system/session idle timeout of 15 minutes.
- Require passwords to be reset at least every ninety (90) days.
- First-time passwords are set to a unique value per user and changed after first use.

3.5 Account and Access Management

3.5.1 Login Security Notice

All computing systems capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

By accessing Discount Tire/America's Tire ("Company") Systems, you agree to the following:

1. comply with the Acceptable Use Policy;
2. consent to authorized Company employees monitoring, intercepting, reviewing, and capturing your activities while using the Company Systems;
3. evidence of unauthorized use, or violation of the Acceptable Use Policy, may result in disciplinary action, including termination;
4. evidence of criminal activity will be reported to law enforcement;
5. all content of the Systems is the property of the Company; and,
6. you should have no expectation of Privacy when using Company Systems.

4. PAYMENT CARD INFORMATION (PCI) RETENTION AND DISPOSAL POLICY

4.1 Policy Applicability

All employees, contractors, consultants, and vendors who use, maintain, or handle Company Payment Card Information (PCI) must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

4.2 Retention Requirements

All PCI, regardless of storage location, will be retained only as long as required for legal, regulatory, and business requirements as outlined in the Discount Tire *Records & Information Management Policy*. The specific retention length will be documented in the Discount Tire *Records Retention Schedule*. PCI "authorization data," including track, CVV2, and PIN information, can and will only be retained only until completion of the transaction. No other storage or retention of credit card data shall occur within the Discount Tire Network. Furthermore, all PCI system and network audit logs must be retained for one (1) year, with ninety (90) days kept available for online use.

4.3 Disposal Process

When no longer needed for legal, regulatory, or business reasons, remove all PCI from the Company's systems and storage media using the approved methods outlined below.

Systems decommissioned or repurposed must have PCI deleted securely by a "wiping" utility approved by the Information Security Team.

Media containing PCI that should no longer be retained must be disposed of in a secure and safe manner as noted below:

- Hard disks: sanitize (7-pass binary wipe), degauss or destroy the platter surface
- Tape media: degauss, shred, incinerate, pulverize or melt
- External USB drives, smart cards, digital media: incinerate, pulverize, or melt
- Optical disks (CDs and DVDs): destroy optical surface, incinerate, pulverize, shred or melt

Before computer or communications equipment can be sent to a vendor for trade-in, servicing, or disposal, a signed "Vendor Form" must be on file. The equipment must be transported in an approved format. Removable computer storage media such as floppy or optical disks, or magnetic tapes may not be donated to charity or otherwise recycled.

Outsourced destruction of media containing PCI must use a bonded Disposal Vendor that provides a "Certificate of Destruction." The Certificates of Destruction need to be maintained, tracked, and stored centrally by the Regulatory Compliance Team or Records Management.

5. PAPER AND ELECTRONIC MEDIA POLICIES FOR PCI

5.1 Policy Applicability

All employees handling hardcopy or electronic media must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

5.2 Storage

5.2.1 Hardcopy Media

Hard copy material containing PCI (e.g., paper receipts, paper reports, faxes, etc.) is subject to the following storage guidelines:

- Will be physically retained in a safe or Security Team approved locking file cabinet within the Company's secure office environments or Security Team approved off-site storage facility.
- Will be retained only for the minimum time deemed necessary for their use.
- Will never be left unattended in employee desks or open workspaces.
- Media will be sent by secured courier or other delivery method that can be accurately tracked.

5.2.2 Electronic Media

Electronic media containing PCI is subject to the following storage guidelines:

- Will never be copied onto removable media without authorization from the Security Team.
- Will be clearly labeled as PCI.
- Will be physically retained in a safe or Information Security Team approved locking file cabinet within the Company's secure office environments or approved off-site storage facility.
- Will be retained only for the minimum time deemed necessary for their use.
- Will never be left unattended in employee desks or open workspaces.

5.3 Destruction

Employees should make every effort to crosscut, shred or place in locked shred bins any printed material containing PCI.

Electronic media must be destroyed as outlined in Section 4.3 of this policy.

6. FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY

6.1 Policy Applicability

All firewalls and routers on the Company's networks, whether managed by employees or by third parties, must follow this policy. Exceptions to this policy will be permitted only if approved in advance and in writing by the CIO.

6.2 Device Management Responsibilities

Management of all company firewalls and routers shall be a combined effort of the Infrastructure Department and the Security Team.

6.2.1 Infrastructure Department

- Assure that changes to firewall security rules follow all change control policies and procedures.
- Document all firewall security rules and changes.
- Apply hardware and software updates from the firewall vendor(s) after change management acceptance and approval.
- Enable appropriate logging of firewall performance and incidents and perform daily monitoring of the logs.
- Provide access to logs related to the firewalls' health, performance, and security incidents.
- Report network security incidents to Information Security Department immediately upon discovery per *Appendix Q, Incident Response Plan*.
- Monitor the up/down status of the interfaces.
- Assure that there is sufficient redundancy in the infrastructure configuration to maximize uptime and fail-over in case of failure.
- Actively monitor firewall security incidents.
- Conduct periodic review of all firewall policies.

6.2.2 Information Security Department

- In the event of suspected compromise, coordinate appropriate responses per *Appendix Q, Incident Response Plan.*
- Assure that security rules applied to the firewalls are sufficient to protect the Company's networks and Protected Information from external attacks and unauthorized access.
- Assure that security rules applied to the firewalls are sufficient to prevent internal security incidents on the Company's network.
- Review all firewall security rule change requests for policy compliance during the change management process.

6.3 Configuration Changes

Firewall changes detailed below must be put through current Change Control Policy.

- Firewall rule additions, deletions, and modifications with protocols not contained in *System Configuration Standards, Appendix F*.
- Firewall hardware or system modifications.
- Firewall software or system upgrades, patches, or hot fixes.

6.4 Allowed Services

Every connectivity path or service that is not specifically permitted by this policy, with supporting documents issued by the Security Team, must be blocked by the Company's firewalls. The list of currently approved paths and services with justifications is listed in *Appendix F, System Configuration Standards.*

6.5 Allowed Network Connection Paths

All internet based inbound traffic is only permitted to the demilitarized zone (DMZ) network. In all cases, this traffic should be limited to HTTP, HTTPS, and TLS where possible. Perimeter routers should not be configured with a route to internal address space, except the DMZ.

Anti-spoofing technologies must be configured on perimeter devices, denying, or rejecting all traffic with:

- Source IP address matching internally allocated, or company owned address space
- Source IP address matching RFC 1918 address space
- Destination IP address matching RFC 1918 address space

Outbound traffic from internal production systems should be restricted to only required protocols and services.

6.6 Configuration Review

Periodically, the Security Team must review each firewall rule set. The review must include the removal, when merited, of unused or unnecessary access paths. All proposed changes identified from this review must go through the Change Control process before implementation.

6.7 Personal Firewalls

All devices that have a direct connectivity to the Internet (e.g., laptops used by employees), and that are used to access the Company's network, must have personal firewall software installed and activated.

All such software must have a non-user-alterable configuration.

7. SYSTEM CONFIGURATION POLICY

7.1 Policy Applicability

All servers and network devices on the Company's network which store, process, transmit or have unrestricted access to the Company's systems or information, whether managed by employees or by third parties, must be built and deployed in accordance with this policy. Departures from this policy will be permitted only if approved in advance, and in writing, by the CIO.

7.2 System Build and Deployment

7.2.1 System Purpose

All computing systems should be designated for a single primary function unless approved by the Security Team (e.g., web servers, database servers, and DNS should be implemented on separate servers).

7.2.2 System Configuration Standards and Processes

All systems, prior to deployment in the production environment, must conform to the *System Configuration Standards, Appendix F,* and applicable processes.

A valid business justification must exist for all deviations from the Company's published configuration standards and/or processes. Any such deviations require written approval by the Security Team.

7.3 Vulnerability Identification and System Updates

7.3.1 Vulnerability Identification

The Regulatory Compliance Team must be informed of information security issues and vulnerabilities applicable to the Company's computing systems. When security issues are identified, the Security Team is responsible for notifying appropriate personnel. Security vulnerability tools and scanners are to be utilized by approved Information Security Team personnel only.

The primary method for identifying new threats as they arise will be through vendor and security-specific Internet mailing lists. Although not complete, the following lists should be subscribed to as well as other vendor lists applicable to the Company's specific software packages and systems:

- aws.amazon.com/security/security-bulletins/
- www.cisco.com
- www.microsoft.com
- IBM Support site: Fix Central
- CERT
- CISA
- NT BUGTRAQ
- SANS
- Red Hat Network

The Company's *System Configuration Standards, Appendix F, must* be updated to reflect measures required for protection from any newly discovered vulnerability. Vulnerabilities may include insecure communication protocols; risk identified as 'high' or 'critical;' improper access control such as directory traversal; cross-site request forgery, etc.

7.3.2 Scanning and Audit

In addition to the above informational alerts, the Security Team is responsible for conducting periodic internal and external network vulnerability scans and after any significant change in the network (e.g., new system component installations, changes in network topology, product upgrades). This process includes using a wireless analyzer to identify any unauthorized access points.

Additional external vulnerability scans will be performed at least monthly.

Website application penetration tests must be completed at least annually by a qualified third party.

All potential vulnerabilities identified through vulnerability scans and penetration exercises will be communicated to appropriate personnel within the Company for applicability and remediation. All vulnerabilities must be corrected, subject to *Change Control Policy*. Follow-up scans will be initiated to confirm compliance with the Company's security standards.

At least annually, the Security Team will conduct a risk assessment to identify threats or vulnerabilities to ensure that the Company's information is protected.

7.3.3 Security Patch Deployment

All security upgrades, patches and configuration changes identified by the Security Team and found to be applicable to the Company's computing resources must be applied to systems within the following time:

Zero Day patches – applied soon as possible, no later than 30 days

Critical and High patches – applied within 30 days

Medium and Low patches – applied within 60 days

As with any change to the environment, the Change Control Policy must be followed.

8. ANTI-MALWARE POLICY

8.1 Policy Applicability

All systems on the Company's networks, whether managed by employees or by third parties, must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

8.2 Software Configuration

Anti-malware software should be in operation on all systems commonly affected by malicious software such as Microsoft Windows or Macintosh operating systems.

All applicable systems must be configured with Security Team approved anti-malware software. The software must be configured to scan for malware either in real-time or on a scheduled basis, and end users must not be able to configure or disable the software.

8.3 Signature Updates

All systems with anti-malware software must be configured to update signatures daily.

8.4 Software Logging

Anti-malware software must alert Information Technology Department personnel in real-time to the detection of malware.

All logs are reviewed for other system components that appear anomalous. Review any findings for identified exceptions and anomalous characteristics.

Retention of anti-malware software logs will be in accordance with the company *Records Retention Schedule.*

9. BACKUP POLICY

9.1 Policy Applicability

All system and application backups, whether performed by employees or by third parties, must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

9.2 Backup and Retention Schedule

Refer to the company Records Retention Schedule.

Where applicable, backup media for the Company's systems will be relocated to an off-site storage facility where there is a high probability that the media will survive in the event of a disaster.

9.3 Transport

Offline storage media used for archival, or back-up purposes will always be handled and retained in a secured environment so that only company personnel and contracted storage facility personnel can access the media. All media couriers and transport mechanisms must be approved by the Infrastructure Department.

All media that is transferred from one location to another will be logged.

All media containing PCI must be appropriately labeled prior to transfer.

9.4 Audit

All media used will be labeled and assigned a unique ID.

Periodic inventories of all stored media will take place. The Infrastructure Department will compare the Company's list of in-use media with records at the storage facility using the offsite storage facility's media inventory report.

9.5 Media Destruction

Information subject to internal or external review such as internal incident investigation or evaluation for external legal hold is suspended from destruction requirements as outlined in the Company *Records & Information Policy* and *Legal Hold Policy.*

Information on acceptable destruction techniques is detailed in section 4.3 of this policy.

10. ENCRYPTION POLICY

10.1 Encryption Key Management

Protected Information designated as PCI will be encrypted using the following software products:

- QMS: All instructions for key management may be referenced in the QMS User's Guide.

10.1.1 Key Access

Keys used to encrypt, and decrypt Protected Information designated as PCI data must be protected from general access. Only approved custodians have access to key administration.

Access to encryption key administration will only be granted to those custodians specifically requiring access due to job function. All access may only be granted by the CIO. These users must sign the *Encryption Key Custodianship Form, Appendix I* specifying that they understand their key custodian responsibilities.

These forms will be maintained in the employee's file.

10.1.2 Key Knowledge

Encryption keys will be created by the referenced software so there will be no knowledge of the actual keys and key components by anyone employed with the Company.

10.1.3 Key Generation

Only strong encryption keys will be used. Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm. Depending on the encryption scheme in question, the following are minimum length requirements for the encryption keys:

- 3DES – 128 bits
- AES – 256 bits
- RSA – 1024 bits
- Vendor recommendations/best practices for other encryption methodologies.

To prevent unauthorized substitution of keys, physical and logical access to the encryption management tool must be secured.

10.1.4 Key Distribution

Distribution of encrypted keys will follow the defined system configuration and change management processes.

- Cryptographic keys should be stored securely in the fewest possible locations and forms.
- All electronic data encryption keys must be stored per software vendor recommendations with storage of key-encrypting keys being separate from data-encrypting keys within applicable applications.
- All hardcopy data encryption keys must be stored in the Data Center in the secured repository managed by the Information Security Department.

10.1.5 Key Changes and Destruction

All data encryption keys for Protected information designated as PCI must be changed annually or when circumstances dictate a change to maintain encryption or key integrity. The following dictates when a key change is required:

- Periodic: Keys must be changed a minimum of one time per year.

- Suspicious Activity: This change is driven by any activity related to the key process which raises concern regarding the security of the existing key.
- Resource Change: Keys must be changed if a custodian terminates employment and/or if the custodian will no longer provide encryption key management functions.
- Technical Requirement: Keys must be changed if the key in place has become questionable due to a technical issue such as corruption or instability.

10.2 Email Transmission of PCI

Protected Information designated as PCI is never to be sent through any end-user messaging technologies (e.g., email, instant messaging, etc.).

10.3 Encryption of Wireless Networks

PCI sent over wireless networks (e.g., Cellular or Wi-Fi) must adhere to the following requirements:

- Wireless segments sending PCI must be detailed in a current network diagram maintained by Infrastructure.
- Perimeter firewalls or strong network access lists must exist between any wireless networks and environments containing Protected Information.
- Strong cryptography (256 bit minimum) and security protocols such as TLS or IPSEC must be used to safeguard Protected Information during transmission over open, public networks.
- Use of WEP to safeguard Protected Information over open, public networks is prohibited.

11. SPECIAL TECHNOLOGIES USAGE POLICY

11.1 Policy Applicability

All users (e.g., employees, contractors, vendors) of special technologies such as wireless technologies, removable electronic media and PDAs deployed on the Company's networks must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

11.2 Approval

The Information Security Department must explicitly approve any use or deployment of special technologies. All requests to authorize use of special technologies must be logged in a Help Desk ticket for tracking purposes.

11.3 Authentication

Where possible, user authentication must be integrated into the Company's authentication systems. Under no circumstances may the user authentication requirements be less strict than currently defined policies and procedures *(See 3.4.2)*.

All non-console access to the Company networks that contain Protected Information using these technologies must be authenticated via a multi-factor, strong authentication scheme approved by the Security Team.

11.4 Device Identification

All special technologies must be labeled with an asset tag. Correlating contact information and device purpose will be maintained within the Asset Management system.

11.5 Acceptable Use

Acceptable use of the Company's special technologies is limited to activities not restricted by the *Acceptable Use Policy, Appendix A*.

11.6 Permitted Locations for Wi-Fi

Physical access to wireless access points or associated gateways and handheld devices must be restricted.

The Infrastructure Department must authorize the placement of any wireless access points.

11.7 Vendor Maintenance and Support

Remote access methods deployed solely for vendor maintenance and support must remain deactivated until required. A request must be recorded in a Help Desk ticket to activate a remote connection. The remote connection will be deactivated immediately after use. The ticket shall not be closed until the remote connection is deactivated.

11.8 Protected Information Access

If any Protected Information is available through remote connections not covered in 11.8, special precautions must be taken. Controls or contractual obligations such as those restricting copy, paste and print functionality or storage onto mobile devices and removable media may be used.

12. SOFTWARE DEVELOPMENT POLICY

12.1 Policy Applicability

All software development on the Company's computing systems must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

12.2 Development Environment

A development/test environment, separate from the production environment, must be used to evaluate all new software. If the development/test environment has connectivity with the production environment, access controls must be in place to enforce the separation.

PCI, including primary account number (PAN), will not be used for development or testing purposes.

All test data, custom application accounts, usernames, and passwords must be removed at the conclusion of testing, and in all cases before software is moved to a production environment.

Code promotion to the production environment will be accomplished by the Change Control Specialists or Technical Analyst/Administrator. The Software Development Team will not modify code in the production environment.

12.3 Secure Software Development Procedures

12.3.1 Development Lifecycle

Internal and third-party development of proprietary software must include security measures throughout the development lifecycle.

The high-level overview of the security measures taking place within each phase of the Company's development process are as follows:

- **Requirements Analysis –** software development team should determine whether application requirements are inherently insecure.
- **Design** – application components should be planned in a manner consistent with data and network security.
- **Development** – programmer/analysts must consider all application vulnerabilities (e.g., memory bound issues, privilege, and access bypass, etc.).
- **Code Review** – programmer/analysts, not solely the primary programmer/analyst, must conduct code reviews of all new software, specifically in an attempt to identify security issues. Appropriate corrections are implemented prior to release. Code reviews are reviewed and approved by management prior to release.
- **QA Implementation** - implementation should not compromise security controls already in place or introduce new vulnerabilities.
- **QA Testing** - in addition to functional and efficiency testing, all security features of the application should be tested.
- **Documentation** – all application features and implementation documentation should include directions on proper security configurations.
- **Production Implementation** – implementation should not compromise security controls already in place or introduce new vulnerabilities.
- **Postproduction** Validation – in addition to functional and efficiency validation, all security features of the application should be validated.

- **Maintenance** – all future application maintenance should not compromise security controls already in place or introduce new vulnerabilities. Any new code must be reviewed and tested as detailed above.

12.3.2 Web-based Applications

All The Reinalt - Thomas Corporation programmer/analysts will receive current and annual training on secure coding practices. All web development must be done taking the "Open Web Application Security Project" guidelines into account, located at http://www.owasp.org. Specifically, the following vulnerabilities must be considered and checked for during the Code Review and Testing phases:

- Unvalidated input
- Malicious use of user IDs
- Malicious use of account credentials and session cookies
- Cross-site scripting
- Buffer overflows due to unvalidated input and other causes
- SQL injection and other command injection flaws
- Error handling flaws
- Insecure storage
- Denial of service
- Insecure configuration management
- Insecure communications
- Improper access control
- Cross-site request forgery (CSRF)

At least annually and whenever significant modifications have taken place, all web-based applications will be put through an application-specific penetration test.

12.3.3 Application Software for PCI

All internally developed or third-party applications dealing with the processing or retrieval of cardholder information must be configured in a manner that encrypts, masks, or truncates the displayed credit card number. See Obfuscation – Data Protection Matrix on the Knowledge Center for additional information on data classification and obfuscation methods.

If the application is designed for a specific purpose in which the full credit card number must be displayed, approval must be given by the CIO.

A separation of roles between personnel developing/testing and personnel administering/maintaining production environments must exist, verified by Tasks detailed in *Periodic Operational Security Procedures, Appendix N*.

13. INCIDENT RESPONSE POLICY

13.1 Policy Applicability

All security incident responses must follow this policy. Departures from this policy will be permitted only if approved in writing by the CIO.

13.2 Reporting Procedures

The Information Center should be notified immediately of any suspected or confirmed security incident. If it is unclear as to whether a situation should be considered a security incident, the Information Security Department should be contacted to evaluate the situation.

It is imperative that any investigative or corrective action be taken only under the oversight of the Information Security Department to assure the integrity of the incident investigation and recovery process.

- No employee should communicate with anyone outside of their team, the Information Security Department, or corporate officers about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated through the Legal Department.
- Security incidents involving violations of Federal, or state law should be immediately reported to the Security Department, who will collaborate with local police and other law enforcement agencies as necessary to help resolve the incident.
- Document any information you know while waiting for the Security Team to respond to the incident. This must include date, time, and the nature of the incident, if known. Any information you can provide will aid in responding appropriately.

13.3 Automated Security System Notifications

All automated intrusion detection systems within the Company's computing environment, including file integrity checking systems, will be configured to automatically notify the designated Infrastructure Department of any potential compromises or attacks. A member of the Information Security Department will be available 24/7 to support incidents in Incident Response Plan, Appendix Q.

13.4 Incident Severity Identification

The Infrastructure Department will first attempt to determine if a suspected security incident justifies a formal incident response. If it does, the following descriptions should be used to determine what response the Infrastructure Department will take:

Level 1 - One instance of potentially unfriendly activity (e.g., unauthorized telnet, disruptive port scan, etc.).

Level 2 - One instance of a clear attempt to obtain unauthorized information or access (e.g., download password files, access restricted areas, single computer successful malware infection, successful buffer or stack overflow attempt, etc.) or a second Level 1 attack within 24 hours.

Level 3 - Serious attempt (e.g., multi-pronged attack, denial of service attempt, malware outbreak, etc.), actual breach or if the incident involves Protected Information.

13.5 Incident Response Plan and Checklists

Refer to the *Incident Response Plan, Appendix Q*.

13.6 Plan Testing and Training

At least once a year, a mock incident will be initiated to facilitate testing of the current plan. The exact incident to be tested will be at the discretion of the CISO. Once complete, a follow up session, as detailed above, will be held.

All company employees who should have an active role within incident response will be part of the test process.

Personnel with security breach response responsibilities must have sufficient training to respond to breaches in security.

14. EMPLOYEE IDENTIFICATION POLICY

14.1 Policy Applicability

All employees must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

14.2 Employee Requirements

Employees and visitors to the Company's facilities must always display their ID badges. It is every employee's responsibility to keep watch for unknown persons or employees not displaying badges, and report to the security desk.

14.3 Facilities

The Facilities Department must locate the badge creation system in a physically secure environment.

The building, data center, and any other restricted areas must have a *Visitor Log, Appendix M* in place. All visitors must sign the form, including: their name, firm represented, and the employee authorizing physical access (via escort). This log must be retained for three (3) months.

14.4 Badge Assignment Procedure

14.4.1 New Badges

As part of the new hire process, the Security Desk is notified via the Help Desk system of all new employees and onsite contractors requiring ID badges. The direct manager for the employee or contractor will submit ServiceNow ticket to authorize and request the necessary physical access.

The Security Desk will review requested badge access to areas that store Protected Information and decide on whether to issue the badge as listed. Access to environments that contain system components that store, process, or transmit Protected Information such as the Data Center requires approval by the Manager of IT Infrastructure. If approved, the Security Desk will create and issue the badge to the new employee, with only approved access levels.

14.4.2 Visitor Badges

An ID badge with no assigned access rights is provided to visitors by the Security Desk upon request of the visited employee. These badges are clearly distinguishable from assigned employee ID badges.

In no case may a visitor ID badge permit unescorted access to physical areas that store Protected Information.

The employee must escort the visitor to the Security Desk to return the ID badge at the end of the scheduled visit.

14.4.3 Data Center

Access to the Corporate or Alameda data center will be reviewed at least quarterly to ensure access is required.

Access requests will go through the Manager, IT Infrastructure and Security Desk. Access will be provided logically through the Security Desk.

A designated Employee or Security Officer will always escort Contractors, Consultants and Vendors while inside the Corporate or Alameda data center.

14.4.4 Changing Access

All requests for a change in access level must be made directly to the Security Desk by the employee's direct manager via a ServiceNow ticket. If the access request is approved, the Security Desk will make the modifications to badge access.

14.4.5 Revoking Badges

Upon being notified of an employee termination, the Security Desk will immediately disable all badge accesses for the terminated employee. The Human Resources Department and employee manager are responsible for collecting the badge from the terminated user, if possible.

15. MOBILE DEVICES

15.1 Policy Applicability

This policy applies to use of any mobile devices issued by the Company or mobile devices used for Company business. All employees must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

15.2 Policy

All mobile devices containing stored data owned by the Company must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, and cell phones.

Users are not permitted to store Company data on devices not issued by Company, such as storing Company email on a personal cell phone or in a non-corporate-provided email account.

Mobile Devices issued by the Company are issued to people with duties that require them to be in immediate and frequent contact when they are away from their normal locations. Personal use should be limited to minimal and incidental use as defined in the *Acceptable Use Policy, Appendix A.*

Personally owned mobile devices not issued by the Company should not be used for Company business.

15.2.1 Laptops

Laptops will employ full disk encryption with an approved software encryption package. Users should use secure remote access (VPN) to connect via a secure encryption channel into Company data and information systems when not on a trusted network (hotel, coffee shop, airport, etc.).

15.2.2 Mobile Phones

Company data stored on mobile phones are to be stored in company provided applications (Microsoft OneDrive, Outlook, Teams) in a secure fashion. Mobile phones will be managed via a Company provided mobile device management application that will provide the ability to secure the device or perform a remote wipe to preserve the confidentiality, integrity, and availability of Company data.

Company is not responsible for the loss of any personal information that may be present on a Company provided mobile device, such as pictures, memos, contacts, voice mails, etc.

15.2.3 Encryption Keys

All encryption keys and passphrases must meet the complexity requirements described in the Discount Tire Information Security Policy Section 3, where applicable.

15.2.4 Bluetooth

Only pair a mobile device with known, trusted Bluetooth accessories. If prompted to pair with an unknown Bluetooth device, deny the request and report such information to the IT Helpdesk. Bluetooth functionality should be disabled unless a hands-free environment is required.

15.3 Voicemail

Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.

15.4 Loss or Theft

Files containing Protected Information may not be stored on mobile device storage unless contained within a managed application such as OneDrive. Any employee found to have violated this policy

may be subject to disciplinary action that leads to, but may not be limited to, being ineligible for continued use of Company mobile devices.

Mobile device users should maintain possession of the mobile device or lock the device to prevent unauthorized access prior to leaving the device in a secure location.

Lost or stolen equipment shall be reported as soon as possible, but no later than 24 hours after the device was discovered missing, to the IT Help Desk.

15.5 Minimum Standards

The standards described below are the minimum accepted by the Company and are applicable for all issued Company mobile devices in use for Company business. These minimums are considered complimentary to standards detailed in *System Configuration Standards, Appendix F*.

1. Passwords/PINs shall be enabled for each device. Passwords/PINs must have a minimum length of 6 characters.
2. The device shall have the ability to be remotely erased or disabled:
    a. After 10 unsuccessful password attempts.
    b. When reported lost or stolen.
3. The device shall be set to lock after 5 minutes of inactivity.
4. Mobile Device Users are required to receive security awareness training covering use of mobile devices.
5. Protected Information shall not be sent by SMS text.
6. Protected Information shall not be sent by peer-to-peer messaging.
7. Software upgrades and security patches shall be applied in a timely manner when prompted.
8. Personally Owned Devices (BYOD) are not permitted.

16. EXCEPTION REQUEST POLICY AND PROCEDURE

16.1 Policy Applicability

Exceptions to IT Security requirements must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the CIO.

16.2 Exception Request Process

An exception to the Discount Tire Information Security Policy may be granted by the Chief Information Security Officer (CISO) or their designee, for non-compliance with established policy or standard. Exceptions are reviewed and considered on a case-by-case basis and their approval is not guaranteed.

Exceptions that are granted will be for a specific period, not to exceed one year. Upon expiration of the exception, an extension of the exception may be requested/renewed if it is still needed. A new Exception Request will need to be filed for renewal.

The exception request must be submitted on a completed Exception Request Form found in the Appendix to the Discount Tire Information Security Policy. Upon submission of the Exception Request Form, the CISO's office will contact the requester to confirm receipt and request additional information, if needed. Once all required information has been received, the CISO will either grant or deny the request.

Exception Requests will be tracked in the risk register maintained by the Discount Tire Information Security Team.

16.3 Risk Assessment

To properly gauge the impact of a security exception, the system must be assessed for business impact and the risk assessed for likelihood to occur. This should be discussed with an information security subject matter expert to ascertain a risk rating. Below is a Risk Heat Map that should be consulted for reference as part of the Exception Request process.

DISCOUNT TIRE
Cyber Security Risk Scoring Matrix

Likelihood			Consequence Criteria				
			1 – Insignificant Minor nuisance, no monetary loss	**2 – Minor** Less than $50,000	**3 – Moderate** Less than $250,000	**4 – Major** Greater than $1,000,000	**5 – Catastrophic** Greater than $5,000,000
	A.	Almost certain to occur in most circumstances	Medium (M)	High (H)	High (H)	Very High (VH)	Very High (VH)
	B.	Likely to occur frequently	Medium (M)	Medium (M)	High (H)	High (H)	Very High (VH)
	C.	Possible and likely to occur at some time	Low (L)	Medium (M)	High (H)	High (H)	High (H)
	D.	Unlikely to occur but could happen	Low (L)	Low (L)	Medium (M)	Medium (M)	High (H)
	E.	May Occur but only in rare and exceptional circumstances	Low (L)	Low (L)	Medium (M)	Medium (M)	High (H)

17. GLOSSARY

Asset Management System - The maintenance and management of assets by the I.T. Asset Management team.

Business Partners - External companies that work with the Company on an on-going basis, providing services, products, or support.

Cardholder Data - The full magnetic stripe data or the Primary Account Number (PAN) **and** any of the following stored with it: cardholder name or expiration date.

Cardholder Environment - The part of the Company Information Systems that stores, processes, or transmits cardholder data or sensitive authentication data.

Change - A formal process used to ensure a product, service or process is only modified in line with the identified necessary change.

Change Control Committee - A group of people representing all I.T. departments and the Information Security Team who oversee and review the change process and specific change requests.

CIO - Chief Information Officer of the Company

CISO – Chief Information Security Officer of the Company

Contractors and Consultants - An individual working temporarily for the Company to provide services and expertise.

Data - Numerical or other information represented in a form suitable for processing by computer.

Development Department - I.T. Programming; The group responsible for creating, maintaining, and updating software code.

Encryption - Any procedure used in cryptography to convert plain-text into cipher-text to prevent anyone except the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security.

Enterprise Architecture – A team responsible for the designation of architecture standards and best practices for the IT business segment.

Enterprise Security Architecture – A member of the Enterprise Architecture Team responsible for applying security architecture principles and practices to guide organizations through the business, information, process, and technology changes necessary to execute business strategies.

Employee – An individual employed by the Company to provide services and expertise.

Facilities Department - Group responsible for providing physical security and non-I.T. infrastructure support and maintenance.

Firewall - Software, hardware, or a combination of both used to protect network services from other networks.

Help Desk - I.T. Information Center group; provides first line customer support and tier 1 security incident notification.

Information - Data at any stage of processing (input, output, storage, transmission, etc.)

Information Security Policies and Procedures - Formal guidelines that describe the Company's responsibility to secure company information.

Information Security Department - A team responsible for developing security policy, implementing security technologies, and defining security related processes.

Infrastructure Department - Information Technology teams responsible for installation, administration and maintenance of all networks and computing devices, including systems' software and applications.

Masked - Replacing the credit card number with a random value.

Mobile Device – Smartphone, tablet, handheld scanner, or similar device that has cellular network service capabilities for transmitting and/or receiving data on behalf of Discount Tire.

Obfuscation – The process by which data is masked, scrambled, redacted, or encrypted.

PCI DSS – the Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that manage branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. Private label cards – those which aren't part of a major card scheme – are not included in the scope of the PCI DSS.

Payment Card Information (PCI) - Encrypted or unencrypted credit card numbers; data specifically identified as protected by the Information Security Department.

Risk, or Technical Security Assessment - A process to determine vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.

Router - A device that finds the best route between any two networks, even if there are several networks to traverse. Remote sites can be connected using routers over dedicated or switched lines to create WANs. Routers can be configured to act as firewalls.

Security Incident - Any adverse event whereby some aspect of computer security could be threatened; loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples of security incidents include malware found on the network, a stolen laptop or mobile device, credit card information emailed outside the Company, a denial-of-service attack, etc.

ServiceNow – A web-based ticketing system used to request services from the IT Department and capture the IT work portfolio.

Special Technologies - Network devices allowing remote or non-stationary access to the Company's network or servers. Examples include Virtual Private Networks, Virtual Desktop Instances and Wi-Fi.

The Company - The Reinalt – Thomas Corporation (d/b/a Discount Tire / America’s Tire / Discount Tire Direct / Tire Rack).

Truncation - Replacing all but the first six (6) and the last four (4) digits of a card number on software screens, databases, reports, and/or customer invoices. Hidden digits are replaced with ‘x’s. Truncated credit card numbers are not considered PCI, as there is no way to revert to the original card number.

Vendors - An outside resource working for the Company to provide services and expertise.

Malware Signature - A malware signature is a unique string of bits, or the binary pattern, of all or part of malware.

Wireless - Transfer of information over a distance without the use of electrical conductors or "wires".

18. LIST OF APPENDICES

If you need access to any of these appendices, please contact the Information Security Department. (Email: DTC_IT_Information_Security@discounttire.com).

Name	Description
Appendix A Acceptable Use Policy	Also available on the Knowledge Center.
Appendix F System Configuration Standards	Description of standards for system configurations.
Appendix I Encryption Key Custodianship Form (sample form)	Form to record understanding and acceptance of custodianship responsibilities. Filed with Human Resources.
Appendix M Visitor Log (sample form)	Form to track visitors to Corporate office and protected areas. Maintained by Facilities.
Appendix N Periodic Operation Security Procedures	List of security procedures to be conducted, and frequency.
Appendix Q Incident Response Plan	Provides plan for handling information security threats. Also identifies and describes the roles and responsibilities of the Incident Response Team.
Appendix R Security Policy Exception Request	Form for requesting exceptions to established Discount Tire Security Policy requirements.