Security Awareness and Acceptable Use Policy

Purpose

Discount Tire, America's Tire, and Discount Tire Direct (the "Company") provide access to information technology resources, ("Company Technology Resources") which includes computers, networks, and connecting devices, in order to support the Company's mission.

The purpose of this Policy is to outline the acceptable use of Company Technology Resources, and to establish everyone's responsibilities when using Company Technology Resources.

Scope

This Policy applies to anyone who uses Company Technology Resources.

General Use

Access to the Company Technology Resources will only be provided to those individuals with a demonstrated Company business need. Information created and/or transmitted on Company systems is the property of the Company. Authorized Company employees may monitor or audit equipment, systems, and network traffic at any time. In addition, authorized Company employees may need to view the content of email (or other electronic tools) for business purposes. Managers have the authority to request any of their employees' accounts be reset or disabled and be given access to their employees' documents as deemed necessary. There is no expectation of privacy while using Company Technology Resources.

The Company allows the personal use of Company Technology Resources as long it does not interfere with official business, increase cost, introduce risk to Company data and information systems, or embarrass the Company. The Company retains the sole right and discretion to disable or block any use of Company Technology Resources.

Protected and Confidential Information

All necessary steps shall be taken to prevent unauthorized access to Protected and Confidential information as defined by Discount Tire's Information Classification and Control Policy. Mark this information as **PROTECTED** or **CONFIDENTIAL** and store in an approved location. All such data is managed and protected in accordance with applicable law. Protected and Confidential information includes, but is not limited to:

INFORMATION	DEFINITION	EXAMPLE	LABEL AS
Protected	Refers to the most sensitive, regulated business information that is intended for use by the Company	Credit Card Information	**PROTECTED** Do not distribute or make hardcopy or electronic copies.
Confidential	Applies to sensitive business information, such as proprietary Company information and customer and employee personal information that is solely intended for use by the Company	Customer Information Employee Information Company Intellectual Property Profit/Loss Information Business Plans/Strategy	**CONFIDENTIAL** Do not distribute.

Published on: 08/20/07 ver 1.0 Updated on: 08/24/23 ver 2.0

Never leave hardcopy Protected or Confidential information unattended on a desk or open workspace, use a locked file cabinet or safe. Use a cross-cut shredder or approved third party shredding service to dispose of Protected or Confidential Information. Company assets and documents should be secured when used at a remote location.

Passwords

The use of secure credentials is critical to the protection of Company systems. In some instances, multi-factor authentication (MFA) is required to access Company resources. Ultimately, users of Company Technology Resources are responsible for the security of their own credentials. Everyone must:

- Create passwords or passphrases that are complex, (i.e., containing letters, numbers, and special characters).
- Avoid use of personal passwords on Company systems.
- Not copy another individual's password.
- Not disclose their own or anyone else's password or User ID.
- Not allow friends, family, or other household members to use their account.
- Lock their computer when not using (Ctrl-Alt-Delete).

Electronic Communications

- Automatic email forwarding from Company accounts to non-Company accounts, such as a home or personal account, is prohibited.
- Communicate professionally. Use appropriate language and content.
- Do not open email attachments or click on embedded links received from unknown senders or contained in suspicious emails as they may contain or download viruses or malicious software.
- The Company has a team to address social media (Facebook, Twitter, Instagram, Yelp, etc.); only this team is authorized to represent the company on these communication mediums.
- Protected information may not be electronically sent outside the Company without approval from a business segment leader or SVP.

Internet

Company Technology Resources are used to communicate and conduct business. Downloading software from non-Company resources increases security risks by potentially introducing malware, back doors, and mechanisms specifically designed to defeat firewalls and security protections.

- Only install or run IT approved software that will be used for work-related functions.
- Ensure antivirus software is installed and running at all times. If antivirus is not installed, not running, or appears to have a warning message, contact the Information Center.

Physical Security

- Be aware of areas that support direct network access when customers, visitors, or vendors are present (showrooms, conference rooms, bays, etc.).
- Do not allow customers, visitors, or vendors to use Company Technology Resources unattended.
- Do not connect any unauthorized device (e.g., personal laptops, cell phones, thumb drives, etc.) to any part of the Company's internal networking or information systems. Personal smart phones may be connected to guest wireless internet access.

- Information contained on portable computers (e.g., laptops, smart phones) is vulnerable to software threats and theft. Take every precaution to protect this equipment from theft, both on and off premises.

Unacceptable Use

Company Technology Resources systems may not be used to engage in illegal or inappropriate activities. Prohibited activities include, but are not limited to:

- Violating intellectual property rights including, but not limited to, the unauthorized copying or distribution of movies, software, music, images, documents, or other material that is protected by copyright, trademark, patents, or other legal protection.
- Installing unapproved software of any kind, including personal software, on any Company Technology Resources.
- The use of non-standard, unapproved, trial version, or free cloud-based software to develop, store, or transmit company information.
- Disabling computer management tools; including reinstalling or replacing the operating system.
- Disabling or attempting to bypass any anti-virus, firewall or other security related software provided by the Company.
- Intentionally introducing viruses or malicious programs into the Company systems.
- Commercial or business use for the profit of an individual or company external to the Company.
- Sending unsolicited bulk email (spam).
- Viewing or distributing:
  - Sexually explicit materials including, but not limited to, images, comments, or jokes.
  - Material that any reasonable person would find to be defamatory, offensive, harassing, derogatory or disruptive.
  - Material that could offend based on race, color, religion, sex, age, national origin or ancestry, physical or mental disability, veteran status or any other basis protected by federal, state, or local law.
  - Material containing disparaging remarks about employees, clients, competitors, prospects, carriers, or vendors.
- Deliberate unauthorized destruction of Company data or other resources.
- Unauthorized use of a system for which the user has authorized access, including the use of privileged commands on a system by a user not authorized to use such commands and unauthorized access to information owned by someone else.

Contact

Reference the Security Page on the Knowledge Center for additional information. Talk with your Manager, AVP/VP, or call the Support Center if you have any questions or concerns regarding this policy.

Stores: (800) 366-4399 or (480) 606-6007
Corporate/Regions: (877) DTC-INFO (382-4636) or (480) 606-6008 (local)