Authorized Networked Devices

Purpose

The purpose of this policy is to establish guidelines for the authorized use of networked devices at Jerry's Beverage Corporation. This policy is designed to safeguard company data and network infrastructure from unauthorized access and damage, and to ensure that all devices connected to the network comply with the company's security standards.

**Scope**

This policy applies to all employees, contractors, and vendors who use networked devices to access Jerry's Beverage Corporation's network and information systems.

**Content**

### *[Authorization](#_Password_Requirements_)* [*Compliance*](#_Access_Review) *and law enforcement*

### *[Security standards](#_Security_Standards)* [*Enforcement*](#_Enforcement)

### [*Access Control*](#_Account_Lockout)

### *[Prohibited activities.](#_Third-party_vendors)*

**Policy**

*Authorization*

All networked devices used to access Jerry's Beverage Corporation's network must be authorized by the IT department. This includes devices such as laptops, desktops, tablets, smartphones, and any other device that connects to the company's network.

*Security standards*

All authorized networked devices must comply with the company's security standards. This includes installing and maintaining up-to-date antivirus software, applying all software patches and updates in a timely manner, and implementing strong passwords and encryption.

*Access Control*

Access to Jerry's Beverage Corporation's network is granted on a need-to-know basis. Users must not share their login credentials with anyone else, and must log off from their networked devices when they are not in use.

*Prohibited* *activities.*

Users must not engage in any activity that may compromise the security of Jerry's Beverage Corporation's network or data.

This includes but is not limited to:

### Introducing malware or viruses to the network

### Attempting to gain unauthorized access to restricted data or systems.

### Sharing confidential information outside of the company

### Using the network for personal use

### Installing unauthorized software on networked devices

### Reporting Security Incidents

### All security incidents, including suspected breaches or unauthorized access to data, must be reported to the IT department immediately. Users must not attempt to investigate or resolve security incidents on their own.

*Compliance with Laws and Regulations*

All networked devices used to access Jerry's Beverage Corporation's network must comply with all applicable laws, regulations, and industry standards. This includes but is not limited to data protection and privacy laws.

### *Enforcement*

Violations of this policy may result in disciplinary action, up to and including termination of employment. In addition, any unauthorized devices or activities that are discovered will be disconnected from the network and investigated by the IT department.

### *Policy Review*

This policy will be reviewed and updated as necessary to ensure it remains relevant and effective in protecting Jerry's Beverage Corporation's network and data.