User Authentication

Purpose

The purpose of this policy is to establish guidelines for user authentication at Jerry's Beverage Corporation. This policy is designed to safeguard company data and network infrastructure from unauthorized access and to ensure that all users are properly authenticated before accessing the company's network and information systems.

**Scope**

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

**Content**

### *[Password Requirements](#_Password_Requirements_)* [*Access Review*](#_Access_Review)

### *[Multi-Factor Authentication](#_Security_Standards)* [*Enforcement*](#_Enforcement)

### *[Account Lockout](#_Account_Lockout)*

### *[Remote Access](#_Remote_Access)*

### *[Third-party vendors](#_Third-party_vendors)*

**Policy**

*Password Requirements*

All users must create a strong, unique password for their accounts. Passwords must be at least 12 characters long and must include a combination of uppercase and lowercase letters, numbers, and special characters. Passwords must be changed every 90 days, and users must not reuse their previous passwords.

*Multi-Factor Authentication*

### Multi-factor authentication (MFA) must be enabled for all accounts that have access to sensitive data or systems. MFA adds an additional layer of security by requiring users to provide more than one form of authentication, such as a password and a one-time code sent to their mobile device.

*Account Lockout*

Accounts will be locked out after 5 failed login attempts. If an account is locked out, the user must contact the IT department to have the account unlocked.

*Remote Access*

Remote access to Jerry's Beverage Corporation's network and information systems is only permitted through a secure virtual private network (VPN) connection. Users must authenticate themselves through MFA to establish a VPN connection.

### *Third-party vendors*

Third-party vendors or contractors must use their own credentials to access Jerry's Beverage Corporation's network and information systems. Access must be granted on a need-to-know basis, and all third-party access must be monitored and audited.

### *Access Review*

Access to Jerry's Beverage Corporation's network and information systems will be reviewed periodically to ensure that only authorized users have access. Access reviews will be conducted by the IT department and any discrepancies will be reported to management.

### *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.