# PASSWORD POLICY

## PURPOSE

In accordance with industry best practices and applicable compliance regulations, the provider has implemented a range of procedures, policies, and guidelines to protect the confidentiality, integrity, and availability (CIA) of critical client data and computing resources. This Password Policy defines the required standards for password creation, use, and protection across the organization.

---

## PASSWORD REQUIREMENTS

All passwords used to access provider systems, the FDD platform, internal services, or any administrative interfaces must meet the following minimum requirements:

- Must include at least **8 characters**
- Must include at least **1 uppercase letter**
- Must include at least **1 lowercase letter**
- Must include at least **1 symbol**

Passwords must be created in accordance with these standards to maintain adequate system-security levels.

---

## STORAGE OF PASSWORDS

Passwords must **not** be stored in:

- Plaintext files
- Unencrypted documents
- Shared drives
- Any location that is accessible outside the provider

Staff may not store passwords in local files or written notes unless they are stored in a secure, provider-approved password management system.

---

## PASSWORD ROTATION

The provider IT department will notify users when a password requires updating. In general:

- Passwords should be updated periodically
- Passwords must be updated **immediately** if a compromise is suspected

---

# USE OF SHARED PASSWORDS

When a shared password (such as an administrative or service password) must be used, the provider IT department must notify users of:

- The purpose of the shared password
- The systems associated with that password
- The expected lifespan of the password
- Any rotation or expiration details

Shared passwords must be stored and transmitted securely at all times.

---

# RESPONSIBILITIES

### All Users

- Must follow this policy at all times
- Must protect passwords from unauthorized access
- Must report any suspected password compromise immediately

### Provider IT Department

- Enforces password rules and controls
- Notifies users when password changes are required
- Oversees secure storage, reset, and lifecycle management

---

# CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with this policy may result in:

- Suspension of system access
- Disciplinary action
- Additional security monitoring
- Other actions deemed necessary by management