1.0 PURPOSE

The purpose of this policy is to prevent the unauthorized use of company-owned computer workstations and servers by establishing standards for authorizing users IDs, requiring strong passwords, and the protection of all passwords.

2.0 SCOPE

The policy applies to all corporate computers and devices that store corporate information. It applies to all users of the organization's network, using any device that has access to the network.

3.0 POLICY

The frontline defense for accessing a company's computer systems is the traditional user ID and password combination. The user ID/password combination authenticates a user to the system.

The IT Operations Manager has the authority to grant user IDs to company approved users. The Information Security Manager has the authority to approve system administrator level access to any system.

3.1 Roles and Responsibilities

- The IT Operations Manager is responsible for:
  - Drafting an approval form for requesting user IDs.
  - Disabling user accounts that are idle for 3 weeks or more.
  - Disabling user accounts upon notice from Human Resources (for employees) and from the appropriate manager when a temporary worker departs.
- The Information Security Manager is responsible for:
  - Enabling multifactor identification, where practical.
  - Printing and distributing a list of currently active user IDs and their system access for their team to every company manager once every quarter. Ensuring that signed and updated lists are promptly returned and user IDs adjusted as noted.
  - Approving individuals for any type of system administrator access at the workstation, server, or network device levels.
  - Disabling guest accounts on all systems.

- The service desk team members are responsible for:
  - Distributing and receiving user ID request forms.
- All IT team members are responsible for:
  - Immediately changing a password if anyone installs a device that is provided with a password from the manufacturer.

3.2 User ID Management

User IDs that are no longer actively needed will not remain enabled on company data systems as they are open opportunities for an attacker. User IDs that are to be disabled or rescinded:

- Any user ID that is idle for more than 15 days will be automatically disabled. Any ID not used for 60 days will be deleted.
- Upon notice from the Human Resources department that someone has left the company, the IT Operations Manager will immediately disable that account. After 60 days, if a replacement person is not assigned to take over these files and access, the ID will be deleted.
- All temporary employee accounts are set to expire in 12 months. The continuing need for these accounts must be requested from the IT Operations Manager annually.
- Once per calendar quarter, the IT Operations Manager will distribute to each company manager a list of the user IDs associated with their department. The list will also include the access granted to each ID. The managers must promptly update the list, sign it, and return it to the IT Operations Manager.
- Guest accounts are never permitted on company systems.

3.3 Password Management

A password is like a key to the door. It opens a gateway to the various company data stores and applications. Accordingly, each person in possession of a company password is required to safeguard it from disclosure to anyone else, whether within the company or in the general public.

3.3.1 Password complexity

All company-owned workstations and servers must be protected using a user ID and password combination. All passwords must follow these guidelines:

- User passwords must be at least eight characters in length; administrative passwords must be at least 15 characters in length.
- A password cannot be a word or phrase that can be found in any dictionary or a word spelled backwards.
- It must contain at least three out of four from the following: lower case letters, upper case letters, numeric character, and special character (e.g., !@#$%^&).
- Must not be a common pattern found on a standard keyboard or any other common pattern of letters or numbers.
- It must not be based on personal information such as birthdays, addresses, names, etc.

- Tools used for password management complexity checking must be enabled when available. Passwords must pass a threshold of complexity as defined by the IT security manager.

3.3.2 Password confidentiality
It is important to protect the secrecy of passwords. As a user's ID moves through the network and works with various servers, it leaves traces in system and application logs. If someone shares his or her password with another person and that person commits a data breach, as far as the data systems are concerned, it is the first person who did it. The following guidelines must be followed when handling passwords:

- Passwords can never be written down anywhere that is not under lock and key (no sticky notes!).
- Passwords can never be included in unencrypted emails or other form of electronic communications.
- Never reveal your password to anyone over the phone, including help desk personnel.
- Do not share your passwords with assistants, coworkers, family members, or friends. All passwords must be treated as company confidential information.
- Do not use the ''Remember Password'' feature of any application.
- Do not store your passwords in any portable electronic device such as tablets or cell phones.

3.3.3 Password change management
Password changes shall adhere to these guidelines:

A. Whenever a new device is installed that is supplied with a manufacturer's password, that password must be immediately changed.
B. All user account passwords must be changed at least every six months. All administrative level passwords must be changed every three months.
C. Previous passwords cannot be used back for 10 generations. This prevents reusing passwords.
D. Passwords cannot be changed more often that once per week. This prevents cycling through the password change history quickly to result in the same password as before.

3.4 Multifactor Authentication
Where practical, the Information Security Manager will implement multifactor authentication using biometric verification and an individual access card. The use of biometric devices or security tokens can significantly reduce the chances of a successful attack using social engineering.

Multifactor authentication will require from any user:

- Something you know—a password
- Something you have—a security access card
- Something you are—a biometric reading such as a fingerprint or retinal scan

4.0 EXCEPTIONS TO THIS POLICY

Any exceptions to this policy must be approved in advance by the company's IT information security manager.

5.0 POTENTIAL PENALTIES FOR POLICY VIOLATION

- Company employees who violate this policy may be suspended from work without pay for a period of time or discharged.
- Temporary employees will be discharged back to their agencies.

6.0 REVISION HISTORY

Date	Revision #	Description of Change
04/01/17	1.0	Initial creation.

7.0 INQUIRIES

Direct inquiries about this policy to:

George Jenkins, CIO
Our Company, Inc.
2900 Corporate Drive
Columbus, OH 43215

Voice: 614-555-1234
Fax: 614-555-1235
Email: gjenkins@company.com