# Password Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

Passwords are the primary form of user authentication used to grant access to [Company Name]’s information systems. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to [Company Name]’s information systems, and thereby compromising the security of those systems.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

The Password Policy applies to all information systems, information components, and employees of [Company Name], including all temporary or contract workers. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to [Company Name]’s information systems, and thereby compromising the security of those systems.

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, smart phones, tablets, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.
* Cloud services, including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Passwords must be constructed according to set length and complexity requirements. As such, passwords must be [indicate length – suggest 8] characters in length and must include [character type – suggest letters (either upper or lower case), numbers, and special characters] characters.
2. Passwords will have both a minimum and maximum lifespan. As such, passwords must be replaced at a maximum of [indicate interval – suggest 90 days] and at a minimum of [indicate interval – suggest 30 days].
3. Passwords may not be reused any more frequently than every [indicate frequency – suggest 12] password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
4. Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
5. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.