User Password Management Policy Template

DATE: .....

Policy Statement

It’s important that users practice due diligence in controlling access to their systems by protecting their user accounts with passwords that are not easily guessed or deduced.

User passwords are an important aspect of computer security. They’re the front line of protection for user accounts. A poorly chosen user password may result in the compromise of our entire network. Therefore, all employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. This includes:

- contractors
- vendors
- authorised third parties

Thank you,

Paul Adlam CEO

DATE: .....

Purpose

The purpose of this policy is to ensure that security practices are introduced and maintained by all employees with respect to our password-protected information infrastructure.

Scope

Users

This policy applies to all users of Chelsea Theatre's IT systems and services.

IT Assets

The policy applies to all IT systems and services.

Documentation

The documentation shall consist of a Password Management Policy (PMP) and related guidelines.

Document Control

The PMP document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.

Records

Records being generated as part of the PMP shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Distributions and Maintenance

The PMP document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document will be with CEO and system administrators. Subsequent changes and versions of this document shall be controlled.

Privacy

The PMP document shall be considered as "confidential" and shall be made available to the concerned persons with proper access control.

Responsibility

The PMP will all be implemented by the CEO, who:

DATE: .....

1. Implements requirements outlined within the PMP.
2. Has oversight of the process for administering passwords for Chelsea Theatre's systems.
3. Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords.

CEO

1. Grants access and reviews access every year to determine the continued need for access and, if the need continues, re-approves through submission of a System Access Request Form.
2. Prepares policy guidelines for the creation, safeguarding, and control of passwords.
3. Approves access to supervisor passwords and passwords for similar privileged accounts used on our network.

Office Manager

1. Communicates to the users the system access and password requirements outlined in this policy.
2. Informs CEO when access is to be removed.
3. Immediately informs CEO if it's suspected that password has been compromised.
4. Issues and manages passwords for systems and applications under their control in accordance with Chelsea Theatre's policy described below.
5. Issues passwords for privileged accounts to the primary system administrator and no more than one designated alternate system administrator. These passwords will be changed at least every 90 days or when necessary/appropriate due to employment termination, actual or suspected password compromise.

Users

1. Understand their responsibilities for safeguarding passwords.
2. Use all data in accordance with job function and company policy.
3. Understand the consequences of their failure to adhere to statutes and policy governing information resources.
4. Immediately notify the line manager if it's suspected that password has been compromised.

Policy

General

1. The PMP shall ensure that all user accounts are protected by strong passwords or passphrases, and that the strength of the passwords meets the security requirements of the system.

2. The concept of aging shall be used for passwords. Passwords on their expiry shall cease to function by a given date as appropriate.
3. Users shall be educated about password protection and the password policy shall be implemented to ensure that users follow best practices for password protection.
4. IT systems shall be configured to prevent password reuse.
5. For critical information systems, account lockout strategy shall be defined. This shall be based on a risk analysis of the system, as well as the costs to be incurred in case such a strategy is implemented.

Access authorisation requirements

1. Access to resources shall be controlled for each of the systems.Access must be granted by email not verbally.
2. Individuals shall be granted access only to those information systems necessary for the performance of their official duties. Users must receive the line manager's and the Office Manager's approval prior to being granted access to information resources. This requirement includes contracted employees and all other non-personnel who have been granted access.
3. Passwords shall be used on all automated information systems to uniquely identify individual users.
4. Passwords shall not be shared with, used by, or disclosed to others. Generic or group passwords shall not be used.
5. To stop password guessing, an intruder lock-out feature shall suspend accounts after 3 invalid attempts to log on. Manual action by a security system administrator is required to reactivate the ID.

Password parameters

All user and system passwords and passphrases, even those temporarily set for new user accounts, should:

- be at least six characters in length
- consist of a mix of alpha, at least one numeric and special characters
- not be dictionary words from any language
- not be names of children, pets, car registration numbers
- not be portions of associated account names (user ID, log-in name)
- not be character strings (ABC or 123)
- not be simple keyboard patterns

In addition, users are required to select a new password immediately after their initial login.

Passwords must be changed at least every 90 days as appropriate. Previously used passwords may not be re-used.

DATE: .....

Password and account security

1. Password accounts not used for 90 days will be disabled and reviewed for possible deletion. Accounts disabled for 60 days will be deleted.
2. Accounts for contractors shall be disabled on the expiration date of their contract.
3. Lockout policy must be implemented for unsuccessful login attempts. As a good practice, a maximum of 5 login attempts should be allowed. The auto-lock policy for locked accounts must be released after 30 minutes only.
4. Screen-saver passwords must be enabled after 5 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.
5. Passwords for all users, including administrator accounts, must be changed periodically.
6. Administrative account passwords must be changed upon departure of staff who had access to that password (mandatory or voluntary) or suspected compromise of the password. User accounts will be disabled upon departure of personnel (mandatory or voluntary). Users should immediately change their password if they suspect it has been compromised.
7. Vendor or service accounts will be removed from computer systems before deployment.
8. Passwords may not be embedded in automated programs, utilities, or applications, such as autoexec.bat files, batch job files, terminal hotkeys.
9. Passwords may be not visible on a screen, hardcopy printouts, or any other output device.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the CEO

Policy exceptions must describe:

- the nature of the exception
- a reasonable explanation for why the policy exception is required
- any risks created by the policy exception
- evidence of approval by all appropriate parties

Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.

Review of this document: annually by CEO

Next review date 22/02/2025

DATE: .....