skillzminer

Skillzminer Limited
163 Bath Street
Glasgow
G2 4SQ
www.skillzminer.com

Title	Password Policy
Version	1.1
Authorized by	Kirsty Mitchell
Published date	27/6/2022
Next review date	27/6/2023

Purpose

The purpose of this password policy is to establish the framework for administering passwords as part of its efforts to maintain the confidentiality, integrity and availability of Skillzminer information.
Responsibility

Skillzminer management team is responsible for administering, maintaining and updating this policy with the approval of the chief technology officer, chief information officer and/or chief operating officer.
Objectives

The objective of this policy is to provide secure and appropriate access to Skillzminer applications, and to Skillzminer systems and data used, processed, stored, maintained and/or transmitted in and through those information systems.
Strategy and focus

Skillzminer's primary strategy for access control is to securely manage access to systems, networks, applications and data needed by Skillzminer employees and other authorised individuals in the performance of their work. The focus of access control is to define the responsibilities of Skillzminer employees and other authorised individuals in promoting secured and appropriate access to all company systems and IT resources.

Policy

Skillzminer is committed to securing all company information stored or accessed through Skillzminer computers or networks. Access to computer systems is restricted to those employees and non employees authorised for such access, and who have been issued appropriate unique user IDs and passwords. Skillzminer considers passwords to be highly confidential.

Skillzminer will implement, whenever feasible, electronic authenticating passwords to applications, networks and other resources to ease compliance with this policy. IT security teams will evaluate password applications and determine the priority, steps and scheduling for implementation of these tools.

All employees and managers are responsible for complying with this policy. Any individual attempting to or requesting someone else to circumvent security or administrative access controls is in violation of this policy. Furthermore, unauthorised use, alteration, destruction or disclosure of system IDs, passwords or confidential information is considered a computer-related crime and punishable under English and Scottish laws.

Access to applications is made possible using a user ID and password. User IDs may include the employee's number, company email address or other approved configurations. Non employees will be assigned a unique ID number.

Access may be revoked if any aspect of this policy is violated. Other actions up to and including termination of employment may also be taken, depending on the violation.

All users of Skillzminer systems and services are required to adhere to the following rules to use, access, store, process and/or display data acquired from company-owned applications and systems. In addition, contractors and their associated employees and agents must adhere to and agree with the following rules:

1. Access to Skillzminer owned applications and systems is granted solely to conduct legitimate business on behalf of the company.
2. Access to specific system functions and data resources is consistent with each user's scope of employment and job responsibilities.
3. Access requests, including user IDs and passwords, are initiated by written request from company business unit managers who have knowledge about their users' legitimate need to access/change data.
4. Access requests for department users must be approved by applicable company department personnel.
5. User accounts will remain active until a user's employment relationship either changes or terminates, or a period of nonuse of one month is exceeded.
6. Managers, directors and executives are notified of all access changes for their users.
7. All contractors and their associated employees and agents must read, agree and sign the appropriate forms before access to Skillzminer networks and/or systems is permitted, and must adhere to the policies set forth in this document.
8. All requests for new access, changes to existing access or termination of access must be submitted on the required forms with department management approvals and justifications if needed.
9. Skillzminer's senior management team shall be contacted with all requests for access activities, e.g., user ID and/or password requests and/or changes.

Password guidelines

1. Passwords must be a minimum of 10 characters.
2. When an initial password is created for a new user ID, or reset, an individual must change the password at the next logon for applications which enable user-initiated password changes.
3. Skillzminer will force password changes at least every couple of moths on systems accessing sensitive business information.
4. For applications that don't support automatic password changes, users are responsible for initiating the change as above. Exceptions are permitted for automated systems (applications, etc.) that communicate without human interaction (computer-to-computer communication).
5. Passwords should be a combination of alphanumeric characters, numbers and symbols, and should not be easily guessed. Examples of passwords that are not acceptable include user ID, dictionary words, first or last name of user, family member, city, town, street, etc.
6. Enforcement of strong passwords will be automated if this feature is available in an application.
7. Generic user IDs are not permitted at the computer application level.
8. User IDs and passwords or open computer application sessions should not be shared, except on shared workstations.
9. Screensavers with passwords should be used for desktop computers and should be activated after no more than 5 minutes of inactivity.

10. Shared workstations should deploy screensavers, but without password protection. The screensaver should be enabled without requiring a password prompt. An additional exception is allowed for computers in locked offices; password-protected screensavers are not required.
11. Terminals in high-traffic or public areas or with access to confidential information should employ automatic logoff or screensavers with much shorter periods of time (typically 3 minutes).
12. Managers must authorise access, on a need-to-know basis, to information systems for activities within their area of responsibility by contacting the IT help desk.

Password administration

1. Failed login attempts may be recorded and reviewed for follow-up action.
2. Users will be locked out of the system after 3 failed login attempts and must contact the senior management for access resetting. Manager approval may be required to fulfil a password reset request.
3. Access privileges will be reviewed prior to granting access based on factors including job title and function (role-based access) or the individual (user-based access).
4. User IDs, passwords or email accounts are not to be transferred to another individual.
5. New accounts may be obtained by calling the IT help desk. Management approval is required before any account can be created.
1. Noncompliance with this policy

Skillzminer employees and authorised contractors who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures as may be determined by Skillzminer's senior management team.

Management review and audit availability

Skillzminer's executives will review and update this policy on a quarterly basis. As changes to company policies are indicated, Skillzminer's management may initiate a change management request to alter the policy (or policies). All company policies will be available for review during scheduled audits.