Shelter Management Information System (SMIS) Privacy Protocol: Password Management

Effective June 2, 2023

Introduction

This Password Management Protocol defines the objectives, requirements, and standards that all Purchase-of-Service (POS) SMIS Users must adhere to, in a consistent manner, to protect the confidentiality, integrity, and availability of SMIS.

Application

This Protocol *is applicable* to POS staff. Effective June 2, 2023, all SMIS POS Users are required to maintain their SMIS password per the requirements of this Protocol. This requirement will be applied over two phases, as follows:

1. **Phase 1:** As of June 2, 2023, the new requirements will be enforced for all (1) new POS users and (2) existing POS users who initiate a password change.
2. **Phase 2:** In 2023 (date to be determined), the new requirements will be applied to all POS users who have yet to update their password to the new standards. At this time, all passwords that do not meet the new requirements will be automatically expired, forcing a password reset to the new standards.

This Protocol *is not applicable* to City of Toronto staff. City staff are already required to maintain their SMIS password based on the same requirements listed in this document, per the City's Access Control Standards and the City's Password Management Policy. If you are a City staff and would like to learn more about these documents, please visit the " Policies, Standards and Procedures" page on the City's intranet portal.

Definitions

Authentication: The ability for a system (e.g., SMIS) to confirm the identity of a person, based on presented Credentials.

Confidentiality: Defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and property information. A loss of confidentiality is the unauthorized disclosure of information.

Confidential Information: Includes, but is not limited to, privileged information, staff reports, personal information, and any other information that must or may be kept confidential.

Credential: The combination of data that vouches for the identity of a person through some method of authentication (e.g. username + password).

Password Rotation Period: Password rotation refers to the changing/resetting of a password. Limiting the lifespan of a password reduces the risk from and effectiveness of Credential-based attacks and exploits, by reducing the window of time during which a stolen password is valid.

Purchase-of-Service (POS): External agencies that are funded by the City of Toronto's Shelter, Support, and Housing Administration (SSHA) Division to provide services to individuals and families experiencing homelessness.

Shelter Management Information System (SMIS): A web-based information management system that is administered by the City of Toronto's SSHA Division. It is used by both City of Toronto staff and POS staff to provide services to individuals and families experiencing homelessness. The information inputted and stored in SMIS is confidential information and must be protected and secured from unauthorized access in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

SMIS User: An individual who has been assigned a SMIS account and associated Credentials. Passwords are associated with the User's identity.

Password Requirements

As of June 2, 2023, all POS staff are required to maintain their SMIS User Password based on the following requirements. All SMIS Users are responsible for creating and choosing strong passwords. Note that User IDs will continue to be maintained by SSHA administrators.

Requirement #	Password Requirement
1	Minimum length of **12 Characters**
2	Contain **at least 1** number (e.g., 1, 2, 3)
3	Contain **at least 1** special character (e.g., !, @, #, $)
4	Contain **at least 1** uppercase letter (e.g., A, B, C)
5	Contain **at least 1** lowercase letter (e.g., a, b, c)
6	Rotate the password at least every **90 Days** (expires on the 91st day)
7	Must not match any of the User's **10 previously used** passwords
8	Must not include the User's **User ID** in the password

Failure to adhere to these requirements may result, at the City of Toronto’s sole discretion, in revocation of a User's Credentials and/or access to SMIS. It may also result in disciplinary action by the User's Employer. This Protocol serves to supplement the existing SMIS Privacy Guidelines and associated Protocols as well as each User's User Responsibility and Confidentiality Agreement.

Password Confidentiality

Passwords **must not be** written down, displayed, or stored in a location that can be accessed by others, including authorized and/or unauthorized individuals.

In the event of a suspicion or confirmation that account Credentials have been compromised, the User must immediately:

1. Inform their Access Manager(s) and Supervisor to investigate the potential compromise and follow the privacy breach protocol outlined in the SMIS Privacy Guidelines;
2. Inform the Supervisor, Agency Review & Quality Assurance at 416-392-8741 and/or hostels@toronto.ca; and,
3. Change their User password. Compromised Credentials must not be used in the future.

Please direct any questions regarding these guidelines to the Supervisor, Agency Review & Quality Assurance at 416-392-8741 and/or hostels@toronto.ca.