Exhibition Place

Policy Name	Policy Type
Access Control Standards Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

This document defines the standards governing Exhibition Place's ("ExPlace") information technology infrastructure in a manner that protects the integrity and availability of the organization's resources.

Standards are developed and maintained to achieve a collaborative approach that ensures ExPlace software, hardware, and data systems all function smoothly together in a secure environment.

This document is for protecting the informational assets within Exhibition Place's information and communications technology environment.

Application

This standard applies to all individuals using technology provided by ExPlace or authorized to access the ExPlace infrastructure and information technology assets to fulfill their duties and ExPlace's business goals. All ExPlace information and technology assets are subject to these standards, regardless of their use or physical location.

Definitions

Access Rights

Are a set of data defining what services a user is allowed to access. This definition is achieved by assigning the user, identified by their User Identity, to one or more user roles.

Account Owner

Is the individual who has been assigned the account. Credentials are associated with the account holder's identity.

Account Owner Manager

Is within the organizational structure, the person to whom the Account Owner reports.

Authentication

Is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Authorized Users

Are all individuals who have been granted access to the ExPlace's Information Technology Assets.

Availability

Is defined as ensuring timely and reliable access to and use of information by authorized users and systems. A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality

Is 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.

External Party

Is an individual or organization that is a legal entity.

Integrity

Is defined as guarding against improper addition, modification, or destruction of information. Enforcing integrity to preserve the timeliness, accuracy, and completeness of information.

Local Administrator Account

Is the built in local system account generally used to perform Local Administrative tasks on computers before connecting to ExPlace's domain, to image or to troubleshoot network connectivity.

Multi-Factor Authentication

Is sometimes referred to as two-factor authentication or 2FA, is a security enhancement that requires someone to present two pieces of evidence – one's credentials – when logging in to an account. Credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.

Principle of Least Privilege

Is allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Role Manager

The individual that is knowledgeable about which person should be assigned which role within a system.

Segregation of Duty

Addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Segregation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

System Administrator

Implements changes to the access control system.

Third Party System

A software/hardware component developed to be distributed or sold by an entity other than the original vendor of the development platform.

Conditions

Standard

1.0 – Account Management

The discipline of Account Management addresses requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user access rights by following a set of user account management procedures.

1.1 – Account Types

Any account created and maintained by ExPlace must be classified as one of the following:

Account Type	Description
Administrator Account	An account that has administrative or high privileges such as management of a computing system, services, and/or application resources. Examples would be an “Elevated Privilege” account or a Local Administrator account.
Regular User (An account that has not been classified but has access to the City of Toronto internal network, will be defined and set as "Regular User" by default.)	An account that is used by an Exhibition Place user (staff or non-staff member) to access and operate Exhibition Place systems. Such account is usually defined and is a part of the Exhibition Place directory services.
Service Account (Resource Accounts)	An account that is usually created to allow services and/or applications to interact with the operating system without user interface.
Generic User Account	An account that is used by multiple Exhibition Place users.
Public Account	An account that is for users that are not related to the Exhibition Place, usually for public applications and/or services. Public Accounts may be managed outside the Exhibition Place directory services (e.g. local account repository managed by the application).

1.2 – Account Lifecycle Management

1.2.1 – Provisioning

Before creating and enabling an account, an account owner must be identified. The owner will acknowledge the ownership of the new account and will be the "point of contact" for future account-related inquiries. The person associated with the user ID is the account owner.

For service accounts and generic accounts, though there is no person directly associated with the account, there still must be an Exhibition Place staff who is identified as the person responsible for the secure maintenance of the account.

1.2.1.1 – ID Creation

When provisioned, except for generic accounts, usernames must be unique to Exhibition Place environment.

User IDs shall:

1. Not contain information related to job function, location, or job status. Any information related to organization or functions should be linked and not contained in the format of the ID.
2. Not be reused and assigned to a different person or system.
3. Be set to automatically expire or become disabled at the end of the contract for third party staff (contractors, consultants, outsourcing suppliers, etc.). Care must be taken to change this date if the contract is renewed. A review of these IDs by the contracting owner/Business Unit shall be undertaken at least annually to verify their continued need.

1.2.1.2 – Process Controls

Separation of duty must be enforced such that the account requester and credential issuer are separate people.

All access requests and their approval must be documented and stored. A single chain email communication clearly indicating requests and approval is acceptable.

If the account owner must manage their own password:

1. Temporary authentication information must initially be provided. The maximum length of time in which the temporary authentication information will remain valid if the user has not used the account shall not exceed 10 business days.
2. Once the maximum length of time (from the time the credential is issued) has been reached and the user has not applied the temporary credential to the applicable system, the temporary credentials must expire, and the user must reapply for authentication credentials.
3. The account owner is forced to create or change their password upon the first use of the system.
4. The system must ensure that the changed password is different from the temporary password.
5. The password complexity of the temporary password must follow the password complexity requirement of this standard.
6. Any temporary passwords must be sent to the account owner in a manner that protects confidentiality of the authentication credentials.
7. Acknowledgement of the successful receipt of the temporary password must be received by the credential issuer.
8. Each temporary password must be unique.

The account owner must be notified of any changes to their account credentials.

1.2.1.3 – Service and Generic Accounts

Each Service and Generic User account can only be valid on a predefined system or set of systems. The creation of a Generic User account type requires an exception approved by ICT Services management.

1.2.2 – Access Control Reviews

There are two types of access control reviews:

a) **Periodic Review**: A process to review all accounts assigned to both information system and applications/services must be engaged based on the "Mapping of Access Control to Data Sensitivity Classification" section of this standard.
b) **Individual Review**: A review of an individual's accounts must be conducted when the business responsibilities of the individual changes.

Access control reviews must be conducted at least annually on all accounts. In addition, individual reviews must be conducted when individual responsibilities change.

Accounts must be reviewed by the Role Manager.

The reviewer must:

(i) Validate the continued business need for each active account with the resource owner.
(ii) Ensure that application/service account credentials will be disabled when no longer needed.
(iii) Reconcile existing accounts with account access requests, modification requests, and disablement requests.
(iv) Note and initiate the revocation immediately of any access not documented or approved by the account provisioning process.
(v) Access rights assigned to accounts must be reviewed and validated to ensure that the principle of least privilege is enforced.
(vi) Include a review of access rights related updates to identify suspicious activities, with special emphasis on administrative-level privilege that may signal compromised accounts. Examples of suspicious activities include:
    a) Unauthorized changes to existing administrative accounts and privileges;
    b) Creation of new administrative accounts/groups without approval or documentation.

1.2.3 – De-Provisioning or Responsibility Changes

The account owner must notify IT Service Desk when:

a) an account is no longer required for business purposes;
b) the access rights assigned to the account owner must be changed due to the account owner's change in business responsibilities (e.g. change of role, decommission of a system) so that the principle of least privilege is maintained.

In case of a user leaving the organization, when Human Resources department is aware of the departure, they must:

1. Notify IT Service Desk of:

a. The account to be disabled (e.g. network accounts);
b. Who the new owners are of the remaining active accounts (e.g. service accounts).

2. Inform account administrators of all third-party providers to Exhibition Place in which the user had an account, of the user's departure, so that the user's accounts on the third-party systems are disabled.

1.2.3.1 – Process Controls

Segregation of duty must be enforced such that the account owner and the system administrator who manages the credentials or access rights are separate people.

All privilege modification or account disable requests, and their approval must be documented and stored. A single chain email communication clearly indicating requests and approval is acceptable.

Unless notified otherwise, the user's manager will automatically become the active account owner.

Upon notification, accounts that are no longer needed must be disabled immediately.

Accounts that have been disabled must never be re-provisioned. If the user leaves the employment of ExPlace and then returns, a new User ID must be issued.

1.2.4 – Authentication

Every user must authenticate themselves before being granted access to information. Authentication uses:

1. Single factor authentication such as username and password, or
2. Multifactor authentication ("MFA").

On all systems that permit MFA capabilities, MFA shall be enforced regardless of user type.

If multifactor authentication is used, all factors must be bound to the same identity, and the binding is enforced at the time of authentication.

On systems that support integration with external identity providers ("IdP"), single sign-on ("SSO") shall be implemented against Exhibition Place's central identity management to provide unified access controls to users.

The system must enforce that when a maximum number of consecutive failed authentication attempts is reached (e.g. wrong password), access must be temporarily denied for at least 15 minutes (locked account) or until an administrator enables the user ID after successfully validating the user's identity.

Failed authentication attempts should be considered consecutive even if performed from different systems and/or with a considerable time gap.

1.2.5 – Authorization

In cases where a person may perform several roles within a system, the User ID shall be allocated the required level of access rights to effectively carry out these roles.

Before a person may perform several business roles, the business process owner, must ensure that the principle of segregation of duty remains in enforcement or compensating controls are added if segregation of duty cannot be enforced.

1.3 – Role Management

When possible, access rights and controls must be assigned to roles (or groups representing the role) and not to specific user accounts.

Each role/group must be assigned:

a) An owner.
b) The minimum access rights required for business purposes. Provisioning of access rights must be based on the principle of least privilege and must enforce separation-of-duty and need-to-know.

A process to review the role/group permissions and user accounts must be conducted by the group's owner to identify:

(i) Unnecessary access rights to be removed as soon as possible.
(ii) Accounts that are disabled or no longer associated with the specific role to be removed from the group as soon as possible.

2.0 – Password Rules

Any set of credentials within the Exhibition Place environment must include, at minimum, a User ID and a password. All employees who are authorized to access organizational resources are responsible for creating and choosing strong passwords.

2.1 – Password / Phrase Settings

Passwords that are created and assigned to any account within the ExPlace environment must meet the following criteria. Password authentication systems must be able to enforce the following criteria:

Description	Local Administrator Account	Administrator Account (other than Local Administrator Account)	Service Account	All Other Accounts
Min. character length	16	12	32	12
Max. lifetime (expiry) in days	365	60	365	90
Min. lifetime in days	0	0	0	0
Min. non-alphanumeric character (e.g. !@#$)	1	1	1	1
Min. numeric character (e.g. 1234)	1	1	1	1
Min. uppercase character (e.g. ABCD)	1	1	1	1
Min. lowercase character (e.g. abcd)	1	1	1	1
Case sensitive	YES	YES	YES	YES

Bad password practices must be avoided. Passwords must not:

1. Include the User Logon ID.
2. Be a representation of common words/passwords (e.g. P@ssw0rd, 123abc!).
3. Be shared with other users.

Specific policies and/or standards may supersede this, when such policies / standards explicitly state that they supersede this standard. However, if the superseding policy/ standard does not address all the listed attributes, the default value should be taken from the table above.

If multifactor authentication is required (e.g. use of token due to privacy concerns), the use of password can be replaced with an alternative authentication method, such as password-less authentication or biometric authentication (e.g. Windows Hello).

Exceptions to the above will be granted based on technological restrictions (e.g. system cannot support minimum length).

2.2 – Wireless Access

Any WLANs intended for access and use by ExPlace staff for business operations shall be secured with WPA2 Personal/Enterprise or greater key exchange protocols, and 128-bit or stronger encryption keys.

ExPlace’s WLANs shall not provide any direct access to corporate resources and/or applications without the use of ExPlace issued virtual private network (“VPN”) connection.

WLANs must be considered as an untrusted network and treated as such.

2.3 – Remote Access

Secure remote access must be strictly controlled and authorized by ExPlace account owner or service provider. All hosts that are connected to ExPlace’s internal networks via remote access technologies must use the most up-to-date anti-virus software and OS patches.

Access control will be enforced via multifactor authentication (such as one-time password authentication or public/private keys with passphrases).

Employees and contractors with remote access rights must ensure that their personal device or device provided by ExPlace (e.g. workstation, tablet, smartphone) which is remotely connected to Exhibition Place 's corporate network, is not connected to any other network at the same time (i.e. split-tunnelling), with the exception of personal networks that are under the complete control of the user.

Personal equipment that is used to connect to ExPlace 's networks must meet the requirements of ExPlace owned equipment for remote access.

Organizations or individuals who wish to implement non-standard Remote Access solutions to ExPlace’s production network must obtain prior approval from ICT Service management.

2.4 – System Access Control

All vendor-supplied default User ID accounts (e.g. "Administrator" in Windows, "root" in Unix\Linux) shall be deleted, renamed or disabled, and/or the passwords shall be altered before a system can be installed on the Exhibition Place network.

In addition, to detect inappropriate use of these IDs, logs of actual usage must be created and reconciled against authorized activities.

Where vendor-supplied accounts cannot be disabled or removed without also disabling the associated system, and where equivalent access rights cannot be granted to an ID assigned to an individual, every effort must be made to develop compensating controls to maintain individual accountability.

Authentication credentials must be stored separately from application data. Authentication credentials should be stored and processed within a centralized authentication system.

Authentication credentials must be stored and transmitted in a manner that ensures their confidentiality and integrity.

Service Account passwords must not be stored on production systems in plain text.

Passwords for Service Accounts in production systems must be different from their corresponding account in non-production systems.

2.4.1 – System Use Notification

The information system displays an approved, system use notification message before granting system access. The notification informs potential users the following:

1. The user is accessing an Exhibition Place information system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties;
4. Use of the system indicates consent to monitoring and recording.

The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

The system must not display passwords on the screen as they are being entered.

The system must validate the logon information only after all input data is entered. If an error condition is generated, the system must not indicate which part of the log-on data is correct or incorrect.

The information must notify the user, upon successful logon, of the date and time of the last logon.

2.4.2 – Session Control

To prevent unauthorized access to the system, a session lock after 15 minutes of inactivity or upon receiving a request from a user must be initialized.

The information system session lock mechanism, when activated will hide what was previously visible on the screen.

A session lock:

1. Will be in effect until the user re-establishes access using established authentication procedures.
2. Is not a substitute for logging out of the information system.

There must be no concurrent sessions using the same Service Account.

2.4.3 – Logging and Monitoring

All systems that make access control (authentication and authorization) decisions shall record and retain audit-logging information in accordance with records management standards.

Such logs must include:

1. The activity that was performed. Activity logs must not contain personal information or confidential business information.
2. Who or what performed the activity and where or on what system the activity was performed from (subject).
3. When the activity was performed.
4. What was the status (such as success vs. failure), outcome, or result of the activity.
5. Log all successful and unsuccessful log-on attempts.
6. Generate an alert if the maximum number of permitted unsuccessful logon attempts is reached.

2.5 – Use of Information Systems by External Party

Accounts created by ExPlace to be used by third parties (e.g. user account for maintenance, service account for ongoing connectivity) must:

1. Adhere to this standard.
2. First be requested and approved by the system owner and system owner's manager.
3. Have a risk assessment conducted and appropriate access controls established before granting third party access to ExPlace assets.

Accounts created for third parties for remote user access (e.g. maintenance or troubleshooting) must be enabled only after being granted access by the system owner and disabled immediately after third-party activities scheduled for that day have been completed. All activities conducted by third parties must be logged, and their activities reviewed, to ensure what was conducted was what was expected.

Accounts created to be used for external information system connections must have an associated ExPlace owner that is accountable for provision/de-provision accounts as required.

All third parties given access to the ExPlace IT systems must agree to abide and meet ExPlace's information security policies and standards prior to being granted access.

Where relevant, third parties must be asked to provide a copy of their access controls policies/standard and if required, outline measures that they plan to take to ensure ExPlace's data and access to ExPlace's systems remain secure.

2.6 – Use of Third-Party Systems

Connections to external third parties (e.g. support providers, information services providers, managed service providers, third-party cloud service providers) to or from the ExPlace network must be documented, limited to the minimum required to meet purpose of the connection, and approved by the system owner.

Connections to external parties must be established only after the external party's information security posture has been assessed and was found to be meeting with the ExPlace information security requirements based on the accessed information and systems.

2.7 – Use of Cloud Services

The use of cloud services must be assessed by the Office of the CISO to ensure the appropriate application of controls.

Related to access control:

a) User credential/password must be securely stored using appropriate encryption/secure hash with proper salt;
b) Cloud Service Provider must establish un-alterable data audit trail (e.g. logs);
c) Cloud Service Provider must have logging and monitoring capability that allows isolation of an incident to specific clients;
d) Cloud Service Provider must support open standard for identity management (e.g. SAML2, OpenID).

The Cloud Service Provider "must ensure compliance with industry standards as related to security in general (ISO27000) or cloud specific (e.g. ISO27017/27018, Cloud Security Alliance Controls)." Specific to access control are as follows:

1. Access to, and use of, audit tools that interact with ExPlace's information systems must be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.
2. User access policies and procedures must be established, and support business processes and technical controls implemented, for ensuring appropriate identity, privilege management, and access management for all internal Cloud Service Provider staff and customer (tenant) users. These policies, procedures, processes, and measures must incorporate the following:
    a. Procedures, supporting roles, and responsibilities for provisioning and deprovisioning user account privilege managements following the rule of least privilege based on job function.
    b. Business case considerations for higher levels of assurance and multi-factor authentication secrets.
    c. Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., cloud provider sub-contractor and/or other customer (tenant)).
    d. Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)
    e. Account credential lifecycle management from instantiation through revocation.
    f. Account credential and/or identity store minimization or re-use when feasible.
    g. Authentication, authorization, and accounting (AAA) rules for access to data and sessions.
    h. Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions.
    i. Adherence to applicable legal, statutory, or regulatory compliance requirements.
3. User access to diagnostic and configuration ports must be restricted to authorized individuals and applications.

4. Policies and procedures must be established:
    a) To store and manage identity information about every person who accesses the cloud service;
    b) Along with supporting business processes and technical measures implemented, for restricting user access as per defined separation of duties to address business risks associated with a user-role conflict of interest;
    c) For permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.
5. The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to Exhibition Place's information systems and data must be followed by coordinated application of resources to minimize, monitor, and measure the risk of unauthorized or inappropriate access. Compensating controls derived from the risk analysis must be implemented prior to provisioning access.
6. Provisioning user access to data and ExPlace-owned or managed (physical and virtual) applications, infrastructure systems, and network components must be authorized by the Exlace's asset owner prior to access being granted and appropriately restricted. Upon request, the Cloud Service Provider must inform the ExPlace of this user’s access,
7. The Cloud Service Provider must provide the capabilities for ExPlace to conduct periodic (at least once per year) access control reviews of user accounts within the control of the Exhibition Place.
8. Timely de-provisioning (revocation or modification) of user access to data and ExPlace-owned or managed (physical and virtual) applications, infrastructure systems, and network components, must be implemented. Upon request, the Cloud Service Provider must inform ExPlace of these changes, especially if Exhibition Place data is used as part the service and/or ExPlace has some shared responsibility over implementation of control.
9. Internal Cloud Service provider staff or ExPlace user account credentials must be restricted ensuring appropriate identity, privilege management, and access management as per the following:
    a) Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);
    b) Account credential lifecycle management from instantiation through revocation;
    c) Account credential and/or identity store minimization or re-use when feasible;
    d) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets).

Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls must be restricted to authorized users.

2.8 – User Responsibilities

2.8.1 – Protecting Passwords

All users must review and sign off on a password responsibility statement that is applicable to the system that they intend on using. All users, including contractors and vendors with access to ExPlace systems, are responsible for taking the appropriate steps to select and secure their passwords. Do not use the "Remember Password" feature of applications (e.g. web browsers).

Passwords must:

1. Not be shared with anyone.
2. Be treated as sensitive, confidential information.
3. Be transmitted securely.
4. Not be revealed over the phone to anyone without properly validating the person's identity first, to ensure that the person is authorized to receive the information.
5. Not contain hints (e.g. "my family name").
6. Not be shared with anyone, including administrative assistants, executive assistants, and managers, co-workers while on vacation, and family members who are not authorized to have such information.
7. Not be written down or stored anywhere in your office or in a file on a computer system or mobile devices (phone, tablet) without encryption.

Any user suspecting their password may have been compromised must report the incident to IT Help Desk and their supervisor / manager.

The potentially compromised password must immediately be changed. If the compromised credential is related to a privileged account or an account that has access to High-confidentiality data or can modify High-integrity data, the usage of the system by the compromised account must be reviewed to ensure that malicious activities did not occur.

2.8.2 – Use of Access

ExPlace users must never use their "Regular User" accounts to perform administrative tasks, and regular accounts must not be granted administrator privileges. If required, a separate "Administrator Account" must be provisioned to them and privileges granted on the account allow them only to conduct administrative tasks.

This will ensure that the "minimum required privileges" principle is maintained and that a clear audit trail is created. Only account owners, or their delegates, can provide access credentials to a "Generic User Account" – it is the account owner's responsibility to ensure the accessing user will not abuse the credentials.

2.8.3 – Administrator Account Usage

Credentials of an Administrator Account must be protected more diligently than regular accounts (e.g. stronger password, frequent password changes – see Section 4.2 Password Rules). Users must properly logout from a system when finished using an Administrator Account and not wait for automatic logout/lockout.

Administrator accounts must:

1. Be used to log into the network when conducting administrative tasks.

2. Be such that even if a Regular account and an Administrator account are assigned to the same person, their authentication credentials (both User ID and secret credentials) for each account must be different.
3. Only a Local Administrator Account may have local administrator rights to workstations and servers.
4. Never be used to perform regular user tasks (e.g. reading emails, composing documents). Administrator Accounts must enforce least privilege such that regular user tasks cannot be performed.
5. Be limited to the minimum required number of individuals.
6. Never be shared with other users (even other administrators) as activities will be logged and associated with the account owner.
7. Have all their activities logged.

If a user normally does not require administrative access to a system but is required to conduct a task, then the user may only be provided administrative access, after approval from the system owner, and only for the duration required to perform the task. Once the task is completed, the temporary Administrator Account must be disabled, and password changed.

Generic Administrator Accounts must be avoided. If system limitations require the use of generic Administrator Accounts, then an exception can be generated with the approval of ICT Services management. If a generic Administrator Account is used, passwords must be changed every 30 days and immediately after any user no longer requires the use of the generic administrator account.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Related Documents

Information and Technology Acceptable Use Policy

User Account Management SOP

Exhibition Place provides employees with a paid leave of absence when there is a death of a family member.

Application

This policy applies to Permanent Employees, Full-Time Renewable Contract Employees, and Full-Time Non-Union Hourly Employees.

Definitions

Day

A day is defined as 7 hours for employees working 35-hour work week; 7.5 hours for employees working a 37.5-hour work week; 8 hours for employees working a 40-hour work week; and 1.5 days for the employees working twelve 12-hour shifts.

Full-Time Non-Union Hourly Employee

An hourly employee hired for a full-time hourly position within the approved permanent staff complement for Exhibition Place.

Full-Time Renewable Contract Employee

An employee hired to work full-time hours in a position that is not part of the permanent staff complement for Exhibition Place.

Permanent Employee

An employee hired for a full-time permanent position within the approved permanent staff complement for Exhibition Place.

Spouse

The employee's married, common-law, or same-sex partner.

Conditions

Exhibition Place provides employees with a paid leave of absence upon the death and funeral of any of the following family members:

- spouse, including common-law or same-sex spouse
- parents including stepparents and parents of spouse
- children including stepchildren
- brother, and brother of spouse
- sister, and sister of spouse
- son-in-law
- daughter-in-law
- grandparent, including grandparent of spouse

Implementation

Employees must inform their Department/Division Head or designate in writing, of the death, and the dates of bereavement leave. Under normal circumstances, bereavement

leave must be taken between the day of the death and seven (7) calendar days following the funeral.

Employees are required to provide Human Resources with supporting documentation (i.e. death certificate, obituary, funeral home notification, or memorial service).

If the death of a family member occurs during an employee's vacation, the employee will be granted bereavement leave with pay, and the vacation credits will be restored. Employees must advise their Department/Division Head or designate in writing and submit reasonable proof to Human Resources to receive approval for the postponement of the vacation and/or restoration of vacation credits.

If a subsequent death occurs for an employee during the same calendar year, Human Resources will replenish four (4) additional bereavement leave credits in the ADP Time and Attendance Program for the employee.

Exhibition Place

Policy Name	Policy Type
Access Management Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The Access Management Policy defines the policies that all employees, contractors, vendors and/or service providers must adhere to, to protect the confidentiality, integrity and availability of the information and technology assets of Exhibition Place ("ExPlace"). It defines the processes and requirements for user access provisioning and de-provisioning. The requirement for managing passwords, including the creation, distribution, storage, and rotation periods.

Application

This policy applies to all employees, contractors, and third-party vendors who have access to ExPlace's information and communications technology ("ICT") systems.

Definitions

IT Management Team (ITMT)

Consists of the CFO&CS and Director of IT/Telecom/Records & Archives. In the absence of the CFO&CS, authority will be delegated.

Service Account

Service accounts are a special type of non-human privileged account used to execute applications and run automated services, virtual machine instances, and other processes.

Conditions

Access Management

The following necessary activities shall be performed during access reviews:

1.1 - Access Provisioning

Unique user IDs must be created for all account owners. A formal user access provisioning process to create, modify, disable and/or delete user accounts must be implemented. This should include documented authorization from applicable ExPlace management.

1.2 - Shared Accounts

Shared accounts are prohibited. Each user should be given unique credentials.

1.3 - Access De-Provisioning

The access rights of all employees and third-party users to information and technology assets must be deprovisioned and removed immediately upon termination of their employment, contract, or agreement, or adjusted upon change.

Changes to a job role must be reflected in the removal of all access rights that are not approved for the new position.

1.4 - Privileged Accounts

Privileged accounts must only be assigned on a need-to-use basis and must be assigned a different user ID from those used for regular business activities. Privileged or administrator accounts must only be used to conduct privileged tasks. These accounts must not be used to perform 'regular' tasks such as reading emails, browsing websites, or composing documents.

Privileged accounts, including but not limited to administrator accounts, shall only be granted after obtaining approval from the ICT Services management. All approvals for privileged access must be documented, including the reasons for granting access and the duration of authorization. All approvals for privileged access must be documented, including the reasons for granting access and the duration of authorization.

1.5 - Session Timeout

Information systems must retain the session timeout until the user re-establishes access using established authentication procedures. Remote access sessions (e.g., RDP, SSH or Virtual Desktop) must timeout after prescribed period of inactivity (recommend 15 minutes).

1.6 - Account Restrictions

Accounts must be locked after three unsuccessful login attempts. Any account locked out due to invalid logon attempts must be reset by an authorized administrator, or automatically after a predefined wait period for least privileged user accounts. Access must be limited to individuals based on their job function.

1.7 - Default Credentials

Administrator accounts (e.g., root, administrator, etc.) must be changed immediately after initial access to the account(s).

Service account credentials must be changed when employees who know the credentials no longer have a business need for such access or is no longer required after a pre-determined expiry date (e.g., internal transfer or termination of employment).

1.8 - Access Review

Periodic reviews must be conducted for all users, system, applications, or services (e.g., semi-annually). Additional reviews must be performed when a user's business responsibilities change or if a contract is renewed.

For privileged accounts, reviews must be conducted at least annually. The completion of the review must have sign off from ICT Services management to ensure that the review has been completed.

The reviewer must:

- Ensure that accounts that are no longer required are disabled.
- Ensure that redundant accounts have not been issued. Note that admin level accounts are a necessary exception to this provision.
- Ensure that separation of duties and the principle of least privilege is enforced.

- Ensure that elevated privileges (e.g., anything from giving program special access to selected folders on “Finance Share” to administrative access (either to the network or specific applications/systems)) are only assigned when necessary and approved by ExPlace management.

1.9 - Remote Access

All remote access must be through a secure connection such as Virtual Private Network (VPN) or other multi-factor authentication options. Employees must use company-issued and configured devices for remote work and remote access must be logged.

1.10 - Use of Third Party and Cloud Environments

Connections to external third parties must only be granted after the external party's security infrastructure has been assessed to ensure third party has appropriate controls to adequately protect the data. A signed agreement must be in place acknowledging their obligation to comply with ExPlace’s policy.

Provisioning and de-provisioning of access rights to third party systems and cloud environment must be documented. The sections above are also applicable to third party user accounts. Third party accounts must be regularly reviewed.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of ICT resources and access to ExPlace’s information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislation.

Authorized users, and ICT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO’s incident response template.

Exhibition Place

Policy Name	Policy Type
Asset Management Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of the Asset Management Policy is to establish the accountability and responsibility surrounding the use of information and technology assets within Exhibition Place (“ExPlace”).

Authorized Users of information and technology assets as defined must work with ICT Services to ensure information stored on information and technology assets is managed throughout its lifecycle in accordance with the sections detailed below.

Conditions

Acquisition

All new, upgraded, or replaced information and technology assets acquisitions must be approved by ExPlace management. Assets must be recorded and managed within the approved asset register.

Asset Identification

All ExPlace information and technology assets must be clearly identified and recorded in an inventory list. This register should include details such as asset name, model, serial number, purchase date, location and assigned user.

Information and technology assets are any system, service, hardware, and network assets that are owned by or supplied to Authorized Users by the ExPlace. This includes, but is not limited to, desktop computers, monitors, printers, mobile devices, digital projectors, scanners, storage devices, network devices (e.g., switches, routers, modems), software (e.g., Microsoft 365, Adobe), email and business applications (e.g., AutoCAD).

Asset Inventory Review

Ensure that the asset inventory list is maintained and up to date. Any discrepancies or losses must be reported immediately to management.

Asset Use

Assets should only be used for legitimate business purposes. Users are responsible for the proper care of the assets assigned to them. Unauthorized use, removal, or relocation of assets is prohibited.

Deployment

IT Asset tags should be affixed to hardware prior to deployment and updated in the inventory list to reflect user or location assignment of the assets, if applicable.

Disposal

All information and technology assets must be replaced and then decommissioned at the

end of their lifecycles or when they no longer meet the minimum standard. On an exception basis, information and technology assets may be temporarily deferred from decommissioning to allow time to move data from one information and technology asset to its replacement.

Information and technology assets that have been identified for disposal will follow the same procedures as the disposal of electronic and paper records. An itemized list of information and technology assets will require management approval prior to destruction. Authorized Users responsible for the decommissioning and disposal of information and technology assets must complete a disposal certificate.

The disposal company must provide a certificate of destruction.

Decommissioned information and technology assets must be removed from the ExPlace network, and the asset inventory updated accordingly.

Security

All information and technology assets, especially electronic devices, must be protected from unauthorized access.

Passwords and security measures must be in place to safeguard sensitive information.

Physical security measures should be implemented to prevent theft or unauthorized access to premises.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace’s information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges, and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO’s incident response template.

Related Documents

Information and Technology Acceptable Use Policy

Exhibition Place

Policy Name	Policy Type
Credential Compromise SOP Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of this SOP is to provide a structured approach for responding to credential compromises. This procedure aims to protect the confidentiality, integrity, and availability of Exhibition Place ("ExPlace")'s information and technology assets.

Application

This applies to all employees, contractors, vendors, and service providers who have access to ExPlace's information systems.

Definitions

Account Owner

The individual responsible for the management and security of a user account.

Credential Compromise

The unauthorized access or use of credentials (e.g., username and password, PINs) that may lead to unauthorized access to information systems.

Conditions

Procedure

1.1 - Reporting a Credential Compromise

Immediate Action

If an account owner suspects that their credentials have been compromised, they must report it immediately to ICT Services, help@explace.on.ca

416-263-3075.

Notification

The account owner must notify their Manager and ICT Services about the suspected compromise.

1.2 - Investigation and Mitigation

Account Monitoring

ICT Services will monitor the account for any signs of further compromise.

Credential Change

ICT Services will initiate a password reset and revocation of all active sessions immediately upon report.

The user will be instructed to regain access to their account with temporary credentials of which they will change upon login.

Incident Documentation

ICT Services will document the incident, including the actions taken and the outcome.

1.3 - Communication

External Communication

If necessary, ICT Services, via authorized channels, will communicate with external parties, such as vendors or service providers, to address the compromise.

Internal Communication

ICT Services will communicate the incident and the actions taken to relevant stakeholders, including the account owner, their manager, and other affected parties.

Responsibilities

Account Owners

Responsible for reporting any suspicion of credential compromise and taking immediate action to secure the account.

ICT Services

Responsible for investigating and mitigating credential compromises.

Exhibition Place

Policy Name	Policy Type
Credential Management Policy	**Corporate**
Original Date	Revision Date
April 16, 2026	

Policy Statement

The Credential Management Policy defines the objectives, requirements, and standards that all employees, contractors, vendors and/or service providers must adhere to, in order to protect the confidentiality, integrity and availability of Exhibition Place ("ExPlace")'s information and technology assets.
This policy specifically provides:

- The requirements for managing credentials, including the creation, distribution, storage, and rotation periods.
- The account owner's obligation to report a suspicion of a potential user account compromise

Conditions

Credential Requirements

1.1 - Unique Credentials

All ExPlace accounts including internal (e.g., Employees) and external accounts (e.g., Residents, Vendors) on information systems must require unique credentials (username and password, PINs, etc.).
Credentials must not be shared among users, except for generic user accounts for which controls must be in place to avoid instances of credential sprawl. Such credentials must only be shared with authorized individuals.

1.2 - Temporary Credentials

When temporary credentials (e.g., one-time passphrases, PINs, or codes) are required, they must be unique, and users must be required to change it upon the first use of the system to a credential different from the temporary credential.
Additionally, temporary credentials for initial access must expire within a predefined period as defined in Section 4.1.2.1.2 in the Access Control Standards.

1.3 - Credential Reset

Credential reset initiated as part of the forgotten password mechanism must be initiated by the system/application after successful user identity validation (e.g., security questions, verification via email, etc.).

1.4 - Credential Composition

All ExPlace information and technology assets, systems and applications must be configured with complex credentials.

1.5 - Credential Confidentiality

Credentials must not be written down, shared, displayed, and stored in clear text.
Credentials must not be stored in readable form in batch files, automated login scripts and computers without access controls, application source code, or other locations where an unauthorized individual may gain access.

Credentials required to access shared information must not be transmitted at the same time or in the same way as the protected information (e.g., UserID must be sent in a separate message from the message containing password).

1.6 - Credential Compromise

In the event of a suspicion or confirmation that an account has been compromised, the credential(s) to all associated account(s) must be changed immediately. The account must be monitored to investigate potential compromise.
Additionally, compromised credentials must be reported to ExPlace management.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.
Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.
Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.
Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Related Documents

Credential Compromise Response SOP Policy
Access Control Standards Policy

Exhibition Place

Policy Name	Policy Type
Hardening and Configuration Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

This policy establishes the principles and requirements for the effective implementation of hardened and secure configurations for servers and network devices that is owned and/or operated by Exhibition Place (“ExPlace”), as well as Third Parties managing services on behalf of ExPlace.

Systems which are not adequately hardened and run default services and/or default passwords are easier to attack as they offer opportunities for attack. Effective implementation of this policy will minimize unauthorized access to ExPlace’s proprietary information and technology.

This policy covers security configuration requirements to harden systems, infrastructure, and applications both on premises and in third party managed clouds.

The scope of this policy includes the following hosted in ExPlace’s data centres or in public clouds:

- Computers
- Servers
- Application Software
- Network assets including Routers, switches, firewalls, load balancers, etc.
- Databases

Conditions

Hardening Guiding Principles

1.1 - Install System

Install the systems as per the vendor’s Security Best Practices and business requirements.

1.2 - Remove Unnecessary Software and Samples

Most systems come with a variety of software packages to provide functionality to all users. Software that is not going to be used in a particular installation must be removed or uninstalled from the system.

1.3 - Disable or Remove Unnecessary Services

All services which are not going to be used in production must be disabled or removed.

1.4 - Disable or Remove Unnecessary User Accounts

Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used must be removed or disabled.

1.5 - Accounts and Passwords

Refer to Access Management Policy for Managing Accounts.

Implement Secure Ports and Protocols

2.1 - Vendor Security Best Practices

Vendor Security Best Practices must be reviewed at least annually to identify ports, protocols, services that are required and only enable what is necessary.

2.2 - Unencrypted Ports and Protocols

Unencrypted Ports and Protocols (e.g., Telnet, File Transfer Protocol [FTP], LDAP, HTTP) must be disabled. If these services are required, use secure alternatives (e.g., SSH, SFTP, LDAPS, HTTPS).

2.3 - Unnecessary services

Unnecessary services (e.g., Hypertext Transfer Protocol [HTTP], Simple Network Management Protocol [SNMP]) must be disabled.

2.4 - Secure access

Secure access to the console must be enabled, admin ports and admin interfaces must use secure protocols.

2.5 - Routers and switches

Routers and switches must be protected by controlling access lists for remote administration.

Install All Mandatory Security Tools

All mandatory security tools must be installed and configured including a suitable endpoint security software solution to prevent malicious software introducing weaknesses into the system.

Configure Firewall

If the system can run its own firewall, then suitable rules should be configured on the firewall to close all ports not required for production use.

Protecting Sensitive Information

Assets that store, process, or transmit sensitive information must be protected using approved encryption algorithms with key lengths equal to industry standards.

Key/Certificate List

An encryption Key/Certificate List must be created and maintained that includes Certification name, purpose, activation and expiry dates, list of applications, assets using the keys/certificates.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace’s information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges, and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Related Documents

Hardening Standards for Windows 11 Policy

Exhibition Place

Policy Name	Policy Type
Hardening Standards for Windows 11 Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of the Hardening Standards for Windows 11 document is to establish a set of guidelines and best practices for securing Windows 11 systems within Exhibition Place ("ExPlace"). These standards aim to enhance the security posture of Windows 11 by implementing measures that protect against vulnerabilities, reduce the risk of cyber threats, and ensure compliance with industry regulations.

By adhering to these hardening standards, the organization can safeguard its information and communications technology infrastructure, maintain the integrity and confidentiality of sensitive data, and provide a secure environment for its users.

Application

This document applies to all IT systems running Microsoft Windows 11.

Conditions

Standards

These standards are based on the Microsoft Security Baseline.

1.1 - MDM Managed

- For MDM (Intune) managed endpoints, security baseline version **24H2** must be applied via the built in Security Baseline functionality of the MDM.
- All default values noted in https://learn.microsoft.com/en-us/intune/intune-service/protect/security-baseline-settings-mdm-all?pivots=mdm-24h2 are applied.
- Deviations from the baseline are noted in section 3.1.

2.1 - Non-MDM Managed

- Machines that are not MDM (Intune) managed must apply security baseline version 24H2 utilizing the Microsoft Security Compliance Toolkit 1.0.
- All default values noted in https://learn.microsoft.com/en-us/intune/intune-service/protect/security-baseline-settings-mdm-all?pivots=mdm-24h2 are applied.
- Deviations from the baseline are noted in section 3.1.

3.1 - Security Baseline Deviations from Default

Control	Default	Value	Reason
User Account Control Behavior of the Elevation Prompt for Standard Users	Automatically deny elevation requests	Prompt for credentials on the secure desktop	Administrators may require temporary elevation of a process in User Account for troubleshooting or administrative activities on the device

Responsibilities

This standard should be reviewed annually and approved by IT management. The latest version of the security baselines should be utilized as they are published by Microsoft with all deviations from baseline documented in section 3.1 of this document.

Exhibition Place

Policy Name	Policy Type
Mobile Device Management Policy	**Corporate**
Original Date	Revision Date
April 16, 2026	

Policy Statement

The Mobile Device Management Policy document defines the policies and standards that all authorized individuals that use Corporate owned or managed devices are obligated to adhere to for protecting the confidentiality, integrity and availability of the information and technology assets of Exhibition Place (“ExPlace”).

This policy is intended to provide directions on the types of processes and procedures that must be carried out in a consistent manner to ensure that the entity’s mobile devices are adequately protected.

Application

This policy is applicable to all authorized individuals using mobile devices provided by ExPlace, or for authorized individuals accessing the entity's infrastructure, information and technology assets to fulfill their duties and the entity's business goals. All mobile devices are subject to this policy, regardless of their use or physical location.

Refer to Acceptable Use Policy for security requirements related to devices.

Conditions

Device Configuration

1.1 Operating Systems

Mobile devices must be updated regularly to run the latest approved operating system (OS) version and security patches and be managed in accordance with the Vulnerability Management Policy.

1.2 Secure Data Management

All authorized devices comply with the following:

- The mobile device must comply with the City’s standards for connecting to the City’s network to support secure communication channels (e.g. Corporate Wi-Fi or Virtual Private Network) and to protect data confidentiality and integrity in transit. This includes SSL, TLS 1.2, and the minimum OS that should be employed.
- Strong data encryption must be implemented on mobile devices per the Encryption Policy. This must ensure that the device's built-in storage is also encrypted. If this is not achievable, compensating controls must be implemented to preserve the confidentiality, integrity, and availability of the data.
- Removable media must be encrypted or configured to 'Read-Only' if encryption cannot be performed.
- Data stored on devices must not be synchronized with external systems that are not approved by the City (e.g. privately owned PCs or cloud storage systems)

- Mobile devices must be managed in accordance with the Vulnerability Management Standard.
- Removable media must be encrypted or configured to 'Read-Only' if encryption cannot be performed.
- Data stored on devices must not be synchronized with external systems that are not approved by Management (e.g., personal PCs or public cloud storage systems).
- Segregation of Private and Business Usage - Authorized users must use mobile devices in accordance with the Acceptable Use Policy.

Device Maintenance and Handling

Users are responsible for ensuring the physical security of mobile devices and that they are protected per the Acceptable Use Policy.

Users must immediately report the loss or theft of devices to ExPlace Management.

Software and Application Installation

Software and/or application installations on mobile devices are restricted to approved applications required for business purposes and from the official App Stores.

Endpoint protection software must be installed on the device.

Security Compliance, Monitoring, and Review

User and System monitoring must be conducted in accordance with the procedures and principles defined in the Acceptable Use Policy.

Audit Trail/Logging

The activity performed on mobile devices should be logged to identify what has been performed under the account and to hold individuals accountable for their actions. This may be used as forensic evidence in the event of a cyber security incident. To preserve the integrity of the log data, it must not be able to be modified by the user.

Security Management

Mobile devices must be configured such that it will not automatically render mobile codes as they have the potential to cause damage to the system if used maliciously.

All discovered or suspected data breaches that occur on any device used to access information technology resources must be immediately reported to ExPlace management.

All ExPlace owned mobile devices attempting to connect to the corporate network through an unmanaged network (i.e., the Internet) will be subject to the Acceptable Use Policy and other applicable requirements.

Authentication and access requirements must adhere to Access Standards.

Acceptable Use

Tampering with or altering the company-approved operating system (e.g., auto screen lock timer, jailbreaking, unauthorized installation of beta releases or non-approved third-party operating system builds) on the device used to access information and technology assets is prohibited.

In case of a regulatory or legal requirement to examine the mobile device, the employee must surrender the device upon request to ExPlace management.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges, and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Related Documents

Access Control Standards Policy

Information and Technology Acceptable Use Policy

Exhibition Place

Policy Name	Policy Type
Network Segmentation Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

This policy establishes the principles and requirements for the effective implementation of segmentation of Exhibition Place ("ExPlace")'s network. The policy covers segmentation of the network both on premises and in public clouds like Azure and AWS.

By isolating segments, targeted security measures can be applied, making the overall network more resilient against cyber threats. Isolation ensures that any security breach is contained within a single segment, significantly limiting its impact.

Conditions

Use of VLANs

ExPlace will segment its Corporate Network with Virtual Local Area Networks (VLANs) which are logical groupings of hosts in a similar broadcast domain. For example, any application or assets exposed externally over the internet must be in their own segregated zone and traffic to other zones must be strictly controlled through use of firewall rules and access control rules.

VLANs can be created, and membership based on the following purposes:

- **Network location** - Externally exposed over the internet, DMZ or Semi-Trusted Zone, Trusted Zone on the internal network.
- **Function** - VLANs may be created based on functional requirements such as to conduct corporate business, to provide guests wireless access.
- **Compliance** - VLANs may be created based on compliance requirements such as grouping by a specific department subject to compliance requirements. Example a PCI [Payment Card Industry] Zone.
- **Security** - VLANs may be created to protect access to sensitive information and to provide privileged access to ExPlace's information and technology assets. Example databases may be in a separate Database VLAN.

Responsibilities

When creating VLANs an identified IT Manager/MSP will be responsible for managing and configuring it.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Exhibition Place

Policy Name	Policy Type
Password Management Policy	**Corporate**
Original Date	Revision Date
April 16, 2026	

Policy Statement

The purpose of this Password Policy is to establish guidelines for creating, managing, and protecting passwords to ensure the confidentiality, integrity, and availability of Exhibition Place ("ExPlace")'s information and technology assets. This is also applicable to administrative and service accounts.

Definitions

Elevated Account

A separate, restricted account and password used to perform tasks that require Local Administrative privileges such as installing software.

Local Administrator Account and Password

The built in Windows system account generally used to perform Local Administrative tasks on computers before connecting to the domain, to image or to troubleshoot network connectivity.

Service Account

Service accounts are a special type of non-human privileged account used to execute applications and run automated services, virtual machine instances, and other processes.

Standard User Account

A network user ID that allows access to network resources such as the Internet and e-mail. These accounts do not have administrative rights and cannot install software or do other administrative tasks by design.

Conditions

Password Creation

Password requirements may differ depending on the type of account and the privileges they have. All passwords must conform to the Access Control Standards.

Phone and Tablet Passwords

- **iOS** - Phone and tablet passwords can only be numeric and the format will remain the iOS default length of 6 digits.
- **Android** – the minimum 6-character alpha-numeric (password vs pin mode) will be enabled.

Password Storage

- Passwords should not be written down or stored in easily accessible locations.
- Use password management tools for secure storage and retrieval.

- Do not share passwords, even with IT personnel, unless necessary for support reasons.
- Do not utilize password saving features in browser (e.g. “Remember by password”)

Password Transmission

- Use secure protocols (e.g., HTTPS) when transmitting passwords.
- Avoid sending passwords through unsecured channels such as email or messaging apps.

Account Lockout

- Implement account lockout mechanisms after a certain number of unsuccessful login attempts.
- Define a reasonable lockout duration (e.g., 15 minutes) to deter brute-force attacks.

Password Policy Enforcement

All system, user, application, admin, and local accounts must adhere to the Password Policy. If a system or technology limitation prevents compliance, a documented exception must be created and approved by ExPlace management.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace’s information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges, and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO’s incident response template.

Related Documents

Access Control Standards Policy

Exhibition Place

Policy Name	Policy Type
Phishing Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of this Phishing Policy is to establish guidelines and measures to protect Exhibition Place ("ExPlace") from phishing attacks. Phishing poses a significant threat to the security of information systems and sensitive data, and this policy aims to mitigate the risks associated with such attacks.

The proactive implementation of this Phishing Policy is essential in safeguarding ExPlace's information and technology assets. All employees play a critical role in maintaining a secure environment by remaining vigilant and reporting any potential phishing threats promptly.

Application

This policy applies to all employees, contractors, and third-party individuals who have access to ExPlace's information and technology assets.

Condition

Phishing Attacks

To address phishing attacks, all employees must:

- Report any suspicious emails or messages by sending the email as an attachment to help@explace.on.ca immediately or utilizing the Report Phishing button (if available). This includes emails that appear to be from a reputable source but contain suspicious links, attachments, or requests for sensitive information.
- Verify the authenticity of any requests for sensitive information before responding or sharing the information. This includes verifying the identity of the requester and the legitimacy of the request.
- Participate in phishing assessment at least annually.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Exhibition Place

Policy Name	Policy Type
Privileged Access Management Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

To establish the accountability and responsibility surrounding the authorization and use of Elevated or Local Administrative Rights when enhanced access is required to Exhibition Place (“ExPlace”) owned assets.

Conditions

Guiding Principles

- Minimize the scope of elevated rights and grant only the minimum level required to perform Local Administrative tasks as per individual job functions.
- Create separate Elevated Accounts for authorized users.
- Do not permit Standard User accounts to have administrator rights to workstations.
- Restrict Elevated and Local Administrative Accounts for performing authorized administrative functions and not for day-to-day tasks.

Process for Granting Elevated or Local Administrative Rights

- The user must complete the Elevated/Local Administrator Rights Form.
- The user must review and agree to the Terms and Conditions and applicable policies.
- Obtain approval from Supervisor/Manager for IT; OR Supervisor/Manager, plus Divisional Director for non-IT.
- All Elevated/ Local Administrator accounts are re-authorized annually.
- The Approval Authority must confirm and authorize that they still perform the same job functions and require the same Elevated/Local Administrative rights.

Responsibilities

Monitoring Elevated Rights

ExPlace will document Evidence of Approval for all Elevated or Local Administrative access rights granted within ExPlace.

ExPlace will maintain a record of all Elevated or Local Administrative accounts that have been granted by ExPlace, along with the documentation of Evidence of Approval and periodic (annual) review.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the ExPlace management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges, and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislation.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Exhibition Place

Policy Name	Policy Type
Security Awareness and Training Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of this Security Awareness and Training Policy is to establish guidelines and requirements for promoting a secure information environment within Exhibition Place ("ExPlace").

This policy aims to create a culture of awareness and responsibility among employees and:

- Educating employees about the importance of cyber security.
- Provide training on best practices for safeguarding sensitive information.
- Raise awareness about potential security threats and risks.

Application

This policy applies to all employees, contractors, and third-party individuals who have access to ExPlace's information and technology assets.

Conditions

Security Awareness Training

ExPlace shall:

- Schedule security awareness training for all new users (employees, contractors, vendors) of IT resources.
- Schedule security awareness training annually, or upon availability of new training content.
- Schedule security awareness training when new training content becomes available.
- Advise the Office of the Chief Information Security Officer (CISO) on changes to maintain an updated database. Note: this is only applicable if training is administered by the Office of the CISO.
- Keep track of security awareness training completed by calendar year.

Responsibilities

Entity Head - ExPlace must ensure that high priority is given to effective security awareness and training for the workforce.

Users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users must:

- Understand and comply with ExPlace's Security Awareness and Training policy.
- Work with management to meet training requirements.
- Follow up with staff who have not completed the training within the allotted period.
- Apply the knowledge and learnings that was acquired within the day-to-day operations.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the EP management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Exhibition Place

Policy Name	Policy Type
User Account Management SOP Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of this SOP is to outline the procedures for provisioning, modification, and de-provisioning user accounts within the organization. This ensures that user access is granted and revoked in a controlled and secure manner.

Application

This SOP applies to all employees, contractors, and third-party users who require access to Exhibition Place ("ExPlace")'s systems and applications.

Conditions

User Provisioning

1.1 - Requesting Access

The manager submits a Request for IT Equipment for A New Employee form.

The request form includes the user's name, job title, department, and required access levels.

1.2 - Approving Access

ICT Services reviews the request form and verifies the information provided.

The manager approval is granted through the form submission.

1.3 - Creating User Accounts

ICT Services creates the user account in the Exhibition Place Identity Provider (IdP) in standard username scheme of first-initial last-name at explace.on.ca (example JDoe@explace.on.ca).

The user's direct report is notified of their account details and provided with the user's initial login credentials.

1.4 - Initial Setup

The user completes the initial setup, including changing their password and setting up multi-factor authentication (MFA).

ICT Services provides the user with training on how to use the basic systems and applications.

User Modification

2.1 - Requesting Modifications

The manager submits a user modification request to ICT Services.

The request includes the user's name, job title, department, and details of the required modifications.

2.2 - Approving Modifications

ICT Services reviews the request form and verifies the information provided.

The request provided in 4.1 acts as approval for the modification as stated.

2.3 - Implementing Modifications

ICT Services makes the necessary changes to the user account in the relevant systems and applications.

The user and manager is notified of the modifications and provided with any updated account details.

2.4 - Final Steps

ICT Services ensures that all modifications are correctly implemented and that the user's access rights are updated accordingly.

The manager and/or user confirms that the modification process is complete.

User De-Provisioning

3.1 - Requesting De-Provisioning

Human Resources notifies ICT services of user departure and/or account deactivation.

The request form includes the user's name, job title, department, effective date of the revocation and reason for de-provisioning.

3.2 - Approving De-Provisioning

Notification from HR shall act as the approval for the de-provisioning of the user account.

3.3 - Disabling User Accounts

ICT Services disables the user account in the relevant systems and applications.

HR is notified once de-provisioning procedures are complete.

3.4 - Final Steps

ICT Services ensures that all access rights are revoked, and that the user's data is archived in accordance with the applicable data governance and retention policies.

Responsibilities

Human Resources (“HR”)

Responsible for notifying ICT Services of new hire or deactivations.

ICT Services

Responsible for managing user accounts and ensuring compliance with this SOP.

Managers

Responsible for approving user access requests and notifying ICT Services of any changes in user status.

Users

Responsible for adhering to the organization's security policies and reporting any issues related to their accounts.

Exhibition Place

Policy Name	Policy Type
Vulnerability Management Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of this Vulnerability Management Policy is to establish guidelines and procedures for identifying, assessing, prioritizing, and mitigating vulnerabilities within Exhibition Place ("ExPlace")'s information systems to ensure the confidentiality, integrity, and availability of sensitive information.

The policy emphasizes proactive measures, including regular vulnerability scans, risk assessments, and prompt patch management, reflecting ExPlace's commitment to staying ahead of evolving security challenges.

Application

This policy applies to all employees, contractors, and third-party vendors who have access to ExPlace's information and technology assets and must comply with the requirements listed under Conditions.

Definitions

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Management

Vulnerabilities and exposures on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

Conditions

Identification

Regularly scan and assess information systems for vulnerabilities through the following methods.

1.1 - Internal Vulnerability Scans

Internal vulnerability scans on all information and technology assets should be performed on a quarterly basis, or more frequently as required. This should include both credential and non-credential scans.

1.2 - External Vulnerability Scans

Internet-facing applications and network devices shall undergo external vulnerability scans on a quarterly basis, or more frequently as required.

Scan should be requested through the City of Toronto Office of the CISO.

1.3 - Ad-Hoc Scans

Ad-hoc scans (internal/external) shall be conducted after any significant change is made to any critical assets or infrastructure upgrade.

Scan should be requested through the City of Toronto Office of the CISO.

1.4 - Annual Penetration Testing

External penetration testing (internet-facing applications and systems) is performed annually at a minimum and after any significant change to the operating environment (e.g., an operating system (OS) upgrade, a sub-network added to the environment, a web server added to the environment, or to verify that the segmentation methods are operational and effective.

Penetration testing should be requested through the City of Toronto Office of the CISO.

1.5 - Endpoint Protection Software

Information and technology assets must employ malware detection software that will immediately notify the City of Toronto's Security Operations Centre of any potential compromises or malware for triage and escalated to Exhibition Place ICT Services for response. The malware detection software must perform a full system scan on a routine basis as a precautionary control.

Remediation

Prioritize and apply patches or updates in accordance with the severity of the vulnerabilities.

2.1 - Patch Management Applicability

Patch management is applicable to all ExPlace's information and technology assets (e.g., software, OS, firmware, and hardware). This is completed to ensure assets are up-to-date and secure to protect the confidentiality, integrity and availability of the information stored.

2.2 - Implementing Patches by Severity

Patches shall be applied in accordance with their severity and adopting industry best practices.

2.3 - Remediation Tracking

All remediation efforts should be tracked and managed by ExPlace, effectiveness to be reported by City of Toronto Office of the CISO's vulnerability management team.

2.4 - Monitoring / Documenting

The list of vulnerabilities that are unable to be mitigated must be documented and closely monitored and added to an exception document.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the EP management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace's information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO's incident response template.

Exhibition Place

Policy Name	Policy Type
Wireless Network Security Policy	**Corporate**
Original Date	**Revision Date**
April 16, 2026	

Policy Statement

The purpose of this policy is to ensure a secure, reliable wireless network that aligns with the Exhibition Place ("ExPlace")'s objectives and services while safeguarding sensitive information and systems.

This policy outlines the guidelines and procedures for the use and implementation of wireless access points (WAPs) supporting ExPlace.

Application

This policy applies to all users, contractors, and authorized users who have access to ExPlace's wireless network.

Conditions

Authorization and Access

- Access to the wireless network is restricted to staff, show attendees, and exhibitors.
- Approval from ExPlace management must be obtained before connecting any new WAPs to the network, changing wireless network policy, etc.

Security Measures

- All wireless access points must be configured with strong authentication protocols (e.g., WPA3) to protect data transmitted over the wireless network.
- The default usernames and passwords on wireless access points must be changed immediately upon installation.

Network Naming (SSID)

- Standardized SSID naming conventions must be established to ensure easy identification of ExPlace's wireless networks.

Physical Security

- Wireless access points should be physically secured to prevent unauthorized tampering or removal.
- Access points should be installed in areas that minimize signal leakage outside of the EP premises.

Network Monitoring and Logging

- Continuous monitoring of wireless networks will be conducted to detect and respond to any suspicious activities.
- Logs related to wireless access points, including connection attempts and changes in configuration, will be retained to support the investigation of a security incident, inappropriate use of the wireless network or availability issues.

Firmware Updates

- Updates of firmware and software on wireless access points will be applied as they become available to patch for vulnerabilities and improve security.

Guest Network

- If a guest network is implemented, it must be isolated from the ExPlace corporate network.
- Guest access will be granted with restrictions to ensure the security of the ExPlace corporate network and that the Guest network is not used inappropriately.

Compliance

- The implementation and use of wireless access points must comply with all applicable ExPlace cyber security policies and standards.

Responsibilities

Employees and Users

Users are responsible for adhering to this policy and reporting any unauthorized wireless access points or suspicious activities pertaining to the use of the wireless network ExPlace management.

ExPlace Management

- Approve all material changes to the wireless network. For example, adding new WAPs, changes to wireless network security policies and settings.
- Review the configuration changes.

IT Department

- The IT department or MSP is responsible for installing, configuring, maintaining (e.g., apply patches as they become available) and monitoring the wireless network.
- Report any deviations to this policy to ExPlace management. For example, inappropriate use of the wireless network.
- They will conduct regular security assessments and address any vulnerabilities promptly.

Implementation

Policy Approval and Review Schedule

This policy is to be approved by the EP management team and reviewed at least on an annual basis.

Compliance and Violation

Authorized users of IT resources and access to ExPlace’s information and technology assets must comply with these policies.

Non-compliance with these policies may result in disciplinary action up to and including termination of employment, privileges, and/or contract relationship. Investigations of non-compliance will be undertaken with consideration of the rights of the individual under

investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Authorized users, and IT support if applicable, should request clarification through their supervisor if they have any concerns regarding compliance with these policies.

Security breaches or incidents must be reported promptly to ExPlace management using the Office of the CISO’s incident response template.