# TO Live

# FINANCE POLICY

| Title | Effective Date | Policy Number |
|---|---|---|
| Travel and Expenses | January 1, 2018<br>March 31, 2022 | 307 |

## General Expenses

TO Live employees are reimbursed for reasonable expenses when conducting business away from their normal place of work. Employees are expected to manage their travel by using accommodations which are economical and practical.

## Local Carriage

TO Live reimburses travelers for the cost of local carriage (including a tip up to a max of 10%) to and from places of business, hotels, airports or railroad stations in connection with business activities. Travelers must provide vendor receipts for all transportation expenses and the receipt must include the date and amount paid. Limousine services are not permitted.

When possible, full time and part time employees, upon request to their supervisor, should use taxi chits available through TO Live's local carriage account under the following conditions:

- Travel to the employee's home when their shifts ends after 12:30am
- Travel from the employee's home when their shifts starts before 7:00am (9:00am Sundays)
- Tips must not exceed 10% of the value of the taxi ride.
- Chits must be filled out legibly and in full.
- Chits may only be used for travel to/from a TO Live venue and the employee's home unless otherwise previously arranged and approved by departmental VP or designate.
- Taxi chit usage is limited to the GTA area (as per Wikipedia):

  The **Greater Toronto Area**, commonly referred to as the **GTA,** includes the City of Toronto and the regional municipalities of Durham, Halton, Peel, and York. In total, the region contains 25 urban, suburban, and rural municipalities. The Greater Toronto Area begins in Burlington in Halton Region, and extends along Lake Ontario past downtown Toronto eastward to Clarington in Durham Region.

TO Live reserves the right to provide the above noted travel reimbursements through "ride sharing" apps and may limit or phase out the use of taxi chits.

Every effort must be made by the employee to obtain a taxi chit prior to travel. In exceptional circumstances where it is not possible to obtain a taxi chit, the employee will be reimbursed for travel costs by submitting a fully completed taxi chit, following Policy #311 Expense Reimbursement, using the Expense Reimbursement Form.

**Out of Town Expenses**

All out of town work-related travel must be approved in advance by the head of each department. All Senior Staff travel is to be approved by the President & CEO.

**Flight Expenses**

Only Economy class reservations will be permitted for all company-related travel. Upgrades to Business class reservations are not permitted unless they are approved in writing by the VP of Finance & Administration in advance of purchasing the upgrade.

Frequent traveler points accrue to the traveler's personal credit. However, transportation and hotels must be booked to the benefit of TO Live and not for the personal pursuit of travel points to the individual traveler.

**Personal Vehicles**

Personal vehicles may be used by employees for business travel (subject to management discretion) if proper for the convenient, timely and efficient conduct of TO Live business.

In the event that an employee's automobile is damaged (beyond normal wear and tear) or the employee is involved in an automobile accident while traveling on company business, TO Live will reimburse the employee's out-of-pocket deductible from their personal insurance policy up to $1,000. This reimbursement applies only to business travel and does not include the employee's normal commute.

Employees using their automobiles for business must have third party liability insurance in the minimum amount of $1,000,000 per occurrence.

**Mileage**

The use of personal vehicles for business travel will be reimbursed at the rate set by the City of Toronto, inclusive of personal vehicle expenses (gas, oil, insurance, etc.) which are not separately reimbursed.
Mileage between an employee's home and normal place of employment during normal

working hours is not reimbursable. TO Live will follow the mileage rate as set by City of Toronto.

**Accommodations**

Accommodations should be booked by obtaining the most cost-effective room rate and shall not exceed **$500 CDN** per night, unless otherwise pre-approved by your Department Head (approval must accompany Expense Report).

**Out of Town Meal Expenses**

Reasonable meal expenses incurred during business are reimbursable in full, subject the following guidelines:

- gratuities for meals do not exceed 20%;
- a valid itemized receipt showing the date, name and location of the restaurant is required for reimbursement;
- list of attendees if other employees are present, with the bill being paid by the employee having the most seniority in attendance.

**Local Meal Expenses**

Please use the following guidelines for expensing local meal charges:

- meal charges can be expensed if the employee has lunch with the client;
- gratuities for meals do not exceed 20%;
- a valid itemized receipt showing the date, name and location is required for reimbursement; and
- list of attendees if other employees are present, with the bill being paid by the employee having the most seniority in attendance
- meal charges cannot be expensed if the employee has multiple meetings throughout the day in town and has a meal alone.

**Mobile Travel Plans**

Employees traveling outside of Canada with a company-provided mobile phone require a mobile travel plan during the duration of their trip. This can be obtained by sending a request via email to the TO Live IT help desk (ithelpdesk@tolive.com) a minimum of one (1) week in advance of your departure.

**Car Rental**

Rental vehicles may only be used when this mode of travel is deemed more cost-effective than other reasonable methods of transportation.

A compact or mid-size vehicle may be rented by the employee having the most seniority in attendance for business purposes, with advance written approval from the Department Head. A rental of a vehicle larger than a mid-size must be approved in writing by your department Vice President with business rationale provided.

**Per Diems**

Under certain circumstance, a per diem may be provided to employees attending business trips or conferences, replacing the need to submit meal receipts. Meals as part of a conference should be deducted when calculating the per diem. TO Live will follow the per diem rate as prescribed by the City of Toronto.

**Other Reimbursable Travel-Related Expenses**

TO Live reimburses the following expenses listed below in connection with business activities/travel, provided they are necessary and reasonable and supported by an original receipt:

- laundry service during trips 3 consecutive days or longer
- parking (excluding valet)
- printing costs for business purposes
- currency conversion fees
- Wi-Fi charges, where not included in room fee
- In-hotel service charges for use of health club facilities, up to $15 per day

**Non-Reimbursable Expenses**

TO Live will **not** reimburse the following expenses:

- Airline club/lounge fees
- Frequent traveler program costs
- Hotel movie rentals, mini-bar service or other in-room services
- Personal articles (i.e. toiletries, magazines, travel bags/luggage, etc.)
- Personal maintenance services (i.e. barber/hairstylist, manicure/pedicure, etc.)
- Passport fees, including photos
- Alcoholic beverages, unless specifically authorized by your department Vice President
- Theft, loss or damage of personal affects.
- Staff social events (birthdays, showers, etc.) are not to be funded from public funds.

Any exceptions to this Travel & Expenses policy requires pre-approval from the VP of Finance & Administration.

# TO Live

# CYBERSECURITY POLICY

| Title | Effective Date | Policy Number |
|---|---|---|
| Security Awareness And Training | September 20, 2023 | 501 |

---

**Last Edited:** February 18, 2024 – David McCracken

**Revision History:**

| | | | |
|---|---|---|---|
| 2023-09-20 | 1.0 | Approved by TO Live | David McCracken |
| 2024-02-18 | 1.1 | Add Revision History + Approved by | David McCracken |
| 2024-02-18 | 1.1 | Add Phishing Section | David McCracken |
| 2025-01-28 | 1.2 | Annual Review | David.McCracken |
| 2025-01-28 | 1.2.1 | Updated to reflect new Reporting Tool | David.McCracken |

This Security Awareness and Training Policy defines the objectives, requirements, and standards that all employees, contractors, vendors and/or service providers are obligated to adhere to for protecting the confidentiality, integrity, and availability of the technology and information assets of TO Live.

This policy has been developed in alignment with cybersecurity best practices (Cyber Centre, NIST, and ISO/IEC 27001/ISO/IEC 27002).

This policy is intended to provide direction on the types of processes and procedures that should be carried out in a consistent manner to ensure TO Live's information technology assets and data are adequately protected and TO Live's cybersecurity objectives are being met.

NOTE: 500 Series Policies contain technical language. Please consult with your Supervisor, Manager, Director, or the Director of Information Technology if clarification is required for all or any part of the 500 Series Policies.

This policy defines TO Live's commitment to cybersecurity, specifically with:

- all users (including third parties) understanding and acknowledging the security policies and applicable standards;
- the cybersecurity awareness and training program that takes into consideration the users' role within TO Live and the specific training required; and
- the required processes and roles and responsibilities to protect TO Live's technology and information resources.

This policy is applicable to all TO Live employees, volunteers and contract employees hired by TO Live using information technology (IT) and operational technology (OT) provided by TO Live, and for accessing TO Live infrastructure, IT assets, OT, and information to fulfill their duties and TO Live's business goals. All TO Live information, including electronic/digital and hardcopy, and technology assets are subject to these policies and standards, regardless of their use or physical location.

**Key Responsibilities**

1. The Information Technology Department will provide a cyber awareness training and phishing program.
2. All employees, contractors, vendors and/or service providers accessing TO Live data are required to complete the cyber awareness training and demonstrate diligence and awareness in the identification of any malicious security threats. The policy may be modified in future to address confirmation requirements.
3. If an employee has any questions and/or requires a deeper explanation, they should contact the Director of Information Technology to obtain clarity.
4. To assist the Director of Information Technology, VPs and Directors are responsible for ensuring that their department staff is compliant with the cyber awareness training requirements through reporting of completion status, and ensure non-compliant users fulfill the required obligations to gain full compliance within their respective departments.
5. The Information Technology Department will establish communication channels to inform applicable employees, contractors, vendors and/or service providers of training requirements and changes to those requirements including any sudden or critical changes to TO Live's threat landscape or other impactful cyber-related news.
6. Simulations of cybersecurity events will be regularly conducted by the Information Technology Department to evaluate users' level of cyber awareness and used as feedback to improve TO Live's cyber awareness program. The test results will be kept as confidential.
7. The cybersecurity awareness and training program shall be reviewed annually to ensure the materials remain relevant to TO Live and reflect the most current legal or regulatory requirements. Under circumstances, such as changes to TO Live's cybersecurity threat landscape, organizational structure, or regulatory requirements, the program shall be updated and communicated with all employees, including third parties, immediately by the Director of Information Technology.

8. The cybersecurity awareness training and phishing program shall consider the risks associated with the users' role within TO Live. Additional training may be required for those users who have cybersecurity-based roles, information owners, and users' who handle sensitive and confidential data. Additional training may also be required for users' who repeatedly fail phishing simulations.

9. All third parties who have access to TO Live's infrastructure, technology, and information assets, and or confidential data shall complete TO Live's cyber awareness training. Depending upon the duration of the third party's contract with TO Live, they shall undergo the cyber awareness training annually as TO Live users must. This will be decided by the Director or Information Technology in conjunction with the departmental VP.

**Phishing**

10. To address phishing attacks, all employees must:

    - Report any suspicious emails or messages by using the Report Phishing Tool within Microsoft Outlook, either desktop or mobile, immediately. This includes emails that appear to be from a reputable source but contain suspicious links, attachments, or requests for sensitive information; and

    - 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; and

    - Participate in phishing exercises at least annually.

**Enforcement of Policy**

11. Prior to using any TO Live infrastructure, IT assets and/or information, authorized users should request a clarification through their Manager, Supervisor, or the Director of Information Technology if they have any concerns regarding compliance with this policy.

12. Security breaches or incidents, suspected or confirmed account compromises, must be reported to the Director of Information Technology immediately.

13. Non-compliance can lead up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with due 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 should request a

clarification through their supervisor if they have any concerns regarding compliance with this policy.

14. TO Live shall ensure compliance with this policy across the organization, with assistance of the Director of Information Technology, by providing direction on individual responsibilities and the specific procedures to be followed. Department VP's and Directors should have a reporting cadence with the Director of Information Technology to confirm that their department employees, contractors, service providers, and vendors are compliant.

# TO Live

# CYBERSECURITY POLICY

| Title | Effective Date | Policy Number |
|---|---|---|
| Personal Passwords | September 20, 2023 | 502 |

---

**Last Edited:** February 18, 2024 – David McCracken

**Revision History:**

| | | | |
|---|---|---|---|
| 2023-09-20 | 1.0 | Approved by TO Live | David McCracken |
| 2024-02-18 | 1.1 | Add Revision History + Approved by | David McCracken |
| 2024-02-18 | 1.1 | Add System/Service section. 5. | David McCracken |
| 2024-02-18 | 1.1 | Add Transmission section. 6. | David McCracken |

This Personal Passwords Policy defines the objectives, requirements, and standards that all employees, contractors, vendors and/or service providers are obligated to adhere to for protecting the confidentiality, integrity, and availability of the technology and information assets of TO Live.

This policy has been developed in alignment with cybersecurity best practices (Cyber Centre, NIST, and ISO/IEC 27001/ISO/IEC 27002).

This policy is intended to provide direction on the types of processes and procedures that should be carried out in a consistent manner to ensure TO Live's information technology assets and data are adequately protected and TO Live's cybersecurity objectives are being met.

NOTE: 500 Series Policies contain technical language. Please consult with your Supervisor, Manager, Director, or the Director of Information Technology if clarification is required for all or any part of the 500 Series Policies.

This policy defines TO Live's commitment to cybersecurity, specifically with:

- the requirements for using personal passwords, including the creation, distribution, storage, and rotation periods; and
- the account owner's obligation to report a suspicion of a potential user account compromise.

This policy is applicable to all TO Live employees, volunteers and contract employees hired by the TO Live using information technology (IT) and operational technology (OT) provided by TO Live, and for accessing TO Live infrastructure, IT assets, OT, and information to fulfill their duties and TO Live's business goals. All TO Live information, including electronic/digital and hardcopy, and technology assets are subject to these policies and standards, regardless of their use or physical location.

**Password Requirements:**

1. TO Live's computer users must abide by this policy, as set out by the Director of Information Technology, as follows:

    - The password format must contain at least twelve (12) characters, and contain at least three (3) of the following four-character groups:

        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Numerals (0 through 9)
        - Non-alphabetic characters (such as !, $, #, @, %).

    - The passwords must adhere to the following:

        - Changed every ninety (90) days.
        - Cannot use previous five (5) passwords.
        - Cannot contain your account or full name.
        - Cannot contain anything related to your job function.

2. Users are responsible for the use of their personal passwords. Unauthorized use, no matter how convenient, could expose the organization to considerable risk and is strictly not permitted.

3. Computer users can change their own password at any time, and are required to do so under the following circumstances:

    - where your password has been revealed to another individual; and
    - at any time where the password has been, or is suspected to be, discovered by another individual; or
    - suspicion that the account pertaining to the password is compromised.

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

5. All system/service, user, applications, admin, and local accounts must adhere to the Password Policy.

6. 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. Suspected or confirmed compromised credentials must not be re-used in the future.

7. Transmission of Passwords must only be done over secure protocols such as HTTPS. Passwords must not be sent through unsecured channels such as email or messaging applications.

**Enforcement of Policy**

8. Prior to using any TO Live infrastructure, IT assets and/or information, authorized users should request a clarification through their Manager, Supervisor, or the Director of Information Technology if they have any concerns regarding compliance with this policy.

9. Security breaches or incidents, suspected or confirmed account compromises, must be reported immediately to the Director of Information Technology.

10. Non-compliance can lead up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with due 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 should request a clarification through their supervisor if they have any concerns regarding compliance with this policy.

11. TO Live shall ensure compliance with this policy across the organization, with assistance of the Director of Information Technology, by providing direction on individual responsibilities and the specific procedures to be followed. Department VP’s and Directors should have a reporting cadence with the Director of Information Technology to confirm that their department employees, contractors, service providers, and vendors are compliant.

# TO Live

# CYBERSECURITY POLICY

| Title | Effective Date | Policy Number |
|---|---|---|
| Access Management | September 20, 2023 | 506 |

---

**Last Edited:** February 18, 2024 – David McCracken

**Revision History:**

| | | | |
|---|---|---|---|
| 2023-09-20 | 1.0 | Approved by TO Live | David McCracken |
| 2024-02-18 | 1.1 | Add Revision History + Approved by | David McCracken |
| 2024-02-18 | 1.1 | Add section for cross reference to other applicable policies. 16. | David McCracken |
| 2024-02-18 | 1.1 | Add MFA section. 21. | David McCracken |
| 2024-02-18 | 1.1 | Add Privileged/Service section. 22-23. | |

This Access Management Policy defines the objectives, requirements, and standards that all employees, contractors, vendors and/or service providers are obligated to adhere to for protecting the confidentiality, integrity, and availability of the technology and information assets of TO Live.

This policy has been developed in alignment with cybersecurity best practices (Cyber Centre, NIST, and ISO/IEC 27001/ISO/IEC 27002).

This policy is intended to provide direction on the types of processes and procedures that should be carried out in a consistent manner to ensure TO Live's information technology assets and data are adequately protected and TO Live's cybersecurity objectives are being met.

NOTE: 500 Series Policies contain technical language. Please consult with your Supervisor, Manager, Director, or the Director of Information Technology if clarification is required for all or any part of the 500 Series Policies.

This policy defines TO Live's commitment to cybersecurity, specifically with:

- the processes and requirements for user access provisioning and de-provisioning;
- assigning access rights based on the user's job function while enforcing the principle of least privilege and separation of duties;
- the approach in achieving secure access to TO Live's information systems and session controls;
- the requirements for managing passwords, including the creation, distribution, storage, and rotation periods;
- the necessary activities to be performed during access reviews; and

- the required processes and roles and responsibilities to protect TO Live's technology and information resources.

This policy is applicable to all TO Live employees, volunteers and contract employees hired by the TO Live using information technology (IT) and operational technology (OT) provided by TO Live, and for accessing TO Live infrastructure, IT assets, OT, and information to fulfill their duties and TO Live's business goals. All TO Live information, including electronic/digital and hardcopy, and technology assets are subject to these policies and standards, regardless of their use or physical location.

**Account Management**

1. Unique user IDs must be assigned to all account owners. The account owner is held accountable for all activities performed under this account. The user ID must not contain the individual's job function, location, or job status.

2. A formal auditable user access provisioning process to create, modify, disable and/or delete (where applicable) user accounts must be maintained by the Information Technology Department.

3. The use of generic user accounts must be limited unless authorized by the Director of Information Technology. In general, this means:

    - Generic administrator accounts must be avoided. If absolutely required, an exception must be generated with documented approval from the Director of Information Technology and sign-off on accepting the associated risks. The account must be disabled, and passwords must be changed immediately once the required task has been performed.
    - Confidentiality of credentials related to generic user accounts shall be maintained (e.g., changing passwords frequently and after any user that no longer requires the use of this account, limiting the number of users that have access to this account).
    - The usage of generic user accounts must be traceable (e.g., automated, system generated logs must be maintained on who accessed the account, access timestamp, access location and reason for access). Manual logs used to track account access is not acceptable.

4. Activities performed on all user accounts (e.g., admin, third party and user accounts) must be monitored and logged. This may include, but not be limited to, log-ons, websites visited, files accessed, files and messages transmitted to and from the account, and the use of software tools. Real-time alerts should be generated for any anomalies.

5. System/Application owners must maintain a centralized inventory for all privileged accounts with access to its systems to ensure traceability and auditability and provide access to them to the Director of Information Technology, as well as notify

the Director of Information of the following:

- accounts that are no longer required;
- end of employment, termination, or change of employment;
- changes to the account owner's job function and/or responsibilities; and
- who the new or remaining owners are of the active accounts.

6. The retention period of users' logging activity data must be maintained in accordance with TO Live's Records Retention Schedule Policy 310.

7. Third party (i.e., consultant/non staff/vendor) user accounts must only be authorized and enabled after the following has been completed:

    - documented approval by Director of Information Technology;
    - a risk assessment to ensure both TO Live and the third party has the appropriate controls in place to adequately protect the data; and
    - a signed agreement by the third party acknowledging their obligations to comply with this policy, any applicable acceptable use procedures (AUPs), and any additional applicable policies or standards.

8. Third party user accounts must be set to automatically expire or to be immediately disabled when no longer needed by the third party. The activities performed by third party user accounts must be tracked and auditable to ensure what was performed vs. what was expected.

9. The access rights of all employees and third-party users to information and assets must be de-provisioned and removed immediately upon termination of their employment, contract, or agreement, or adjusted upon change. Changes to a job role must be reflected in removal of all access rights that were not approved for the new position. Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as whether the termination or change was initiated by the employee, contractor, or third-party user, or by management.

10. Extended access rights can be granted to user accounts only when it is approved by the user's assigned manager and a formal written request submitted to the Director of Information Technology. Prior to granting such requests, due diligence must be performed to verify the identity of the individual and if the request aligns with their job function.

11. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access to the allowed assets and information. Successful and unsuccessful attempts must be logged.

12. Access rights and controls, wherever possible, must be designed and assigned according to job function/role and not to specific user accounts in adherence to Role-Based Access Control (RBAC).

13. Vendor support accounts must only be enabled by the Information Technology Department and approved by the Director of Information Technology when needed and must be disabled immediately after use.

14. Vendor-Supplied Accounts shall be disabled, renamed, or deleted and/or the passwords shall be altered before a system can be installed on any TO Live networks. If this is not feasible without also disabling the associated system(s), compensating measures must be implemented to preserve individual accountability and the integrity of these accounts.

15. 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 may be monitored to investigate potential compromise. Additionally, compromised credentials must not be re-used and the Director of Information Technology notified.

16. Accounts, Credentials, and their usage, are also subject to the following TO Live Policies:

    - Personal Passwords 502
    - Mobile Device Management 504
    - Credential Management 505
    - Access Management 506

**Separation of Duties**

17. Access control roles must be segregated such that no single user can access, modify, or use assets without appropriate authorization or detection. The initiation of an event (e.g., the escalation rights) should be separated from its authorization.

18. The principle of least privilege must be employed, allowing only authorized access privileges which are strictly necessary to accomplish assigned tasks and fulfill role duties as per business requirements.

19. Privileged or administrator accounts must only be assigned on a need-to-use basis and should 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 should not be used to perform 'regular' tasks such as reading emails, browsing websites, or composing documents.

**System Logon Notification**

20. Information systems, where the capability exists, must display privacy and security notices to users before granting access and outline that access is subject to the terms of their employment agreement.

**Multi-Factor Authentication (MFA)**

21. MFA must be used for all Microsoft Office 365 Accounts within TO Live's tenant, including administrative accounts. MFA for third party cloud platforms must be integrated with MFA where possible and setup by the Information Technology Department.

**Privileged and/or Service Accounts**

22. Privileged and/or Service 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.

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

**Secure Access**

24. Validation of authentication information should only be completed once all data has been entered. The system must not indicate to the user which part of the credential is incorrect or display passwords while being entered.

25. Access to information and assets must be granted only after successful user account authorization, authentication, MFA, and encryption.

**Session Control**

26. Information systems must limit the number of concurrent sessions for each user account and/or account type to a defined number, where applicable.
27. Information systems must terminate a user account session after conditions or trigger events requiring session disconnect (e.g., periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions).

28. Information systems must retain the session timeout until the user re-establishes access using established authentication procedures. Remote access sessions must

timeout after ninety (90) minutes of inactivity. Non-remote sessions must time out after fifteen (15) minutes of inactivity.

**Account Restrictions**

29. User accounts must be locked after a maximum of five (5) unsuccessful login attempts. Any account locked out due to invalid login attempts must be reset by the Information Technology Department unless there are provisions defined for self-service or automated password resets. In the event of an automated password reset, the temporary password should be set to expire after thirty (30) minutes. If the user has exceeded the time limit to use the temporary password, they are required to submit another request.

30. Access to system components and data shall be limited to only those individuals whose job requires such access which is determined by:

    - system and data resources that each role needs for their job function;
    - permissions based on job function (read, write, delete, and execute);
    - relevant legislation and/or contractual obligations regarding access to data or services; and
    - level of privilege required (for example, user, administrator, etc.) for accessing resources.

31. Access control system(s) for system components shall restrict access based on a user's need-to-know and set to "deny-all" unless specifically allowed. The access control system(s) should include the following:

    - coverage of all system components;
    - assignment of privileges to individuals based on job classification and function;
    - default "deny-all" setting; and
    - ensure that security policies and operational procedures for restricting access to data are documented, in use, and known to all affected parties.

**Access Review**

32. The Information Technology Department should conduct bi-annual reviews of all accounts to systems and applications or services, in addition to performing reviews when a user's business responsibilities changes, or if a contract is renewed.
33. The Information Technology Department reviewer must:

    - document and immediately revoke any access rights that have not been documented or approved;
    - identify and escalate any suspicious activities performed on the accounts, with special emphasis on administrative or privileged accounts to the Director

of Information Technology. This includes unauthorized changes to a users' access rights and the creation of an account without approval or documentation;
- ensure that redundant IDs have not been issued to others; and
- ensure that separation of duties and the principle of least privilege is enforced.

34. Service account credentials must be changed as soon as possible and within one (1) business week when employees who know the credentials no longer have a business need for such access.

35. Inactive account activity must be logged and acted upon based on the following criteria:

    - After forty-five (45) days of inactivity, the account owner must notify the Director of Information Technology of the inactivity or non-usage.
    - After sixty (60) days of inactivity, the account owner must notify the Director of Information Technology and be aware that the account will be disabled in thirty (30) days if it continues to remain inactive. Re-activation of the disabled account must be requested in writing to the Director of Information Technology.
    - After ninety (90) days of inactivity, the account must be disabled and/or deleted (when applicable) if no issues have been reported. The attributes of the account (e.g., username, access rights, and authentication requirements) must be stored as needed upon deletion. Accounts that cannot be deleted (e.g., accounts within financial applications) must be disabled and managed in accordance with applicable regulatory or business guidelines. Deletion of an account should be evaluated on a case-by-case basis overseen by the Director of Information Technology.

**Remote Access**

36. Remote access must be authorized by the department Director or above and the Director of Information Technology, and the remote access account must require Multi-Factor Authentication (MFA).

37. Users with remote access rights must ensure that the device connected to TO Live’s network is not simultaneously connected to another network (e.g., split tunneling).

38. Remote access must be monitored and logged with records maintained for access allocation and revocation for remote users.

39. Remote access must have preventive controls/mechanisms (i.e., encryption, cryptography, etc.) to protect the confidentiality and integrity of remote sessions.

40. All computers connected to internal networks via remote access technologies must use the most up-to-date endpoint security software as assigned by the Information Technology Department.

**Third Party and Cloud Environments**

41. Provisioning and de-provisioning of access rights to third party systems and cloud environments must be completed and documented by the Information Technology Department.

42. Connections to external third parties must only be granted after the external party's security infrastructure has been assessed by the Director of Information Technology and meets TO Live's security and Access Management Policy 506 requirements.

43. User account credentials must ensure the appropriate identity, privilege management, and access management as per the following:

    - identity verification;
    - service-to-service application (e.g., API);
    - information processing interoperability (e.g., SSO and federation);
    - Authentication, Authorization and Accounting (AAA) rules;
    - enforce the rule of least privilege based on job function; and
    - modify user access rights, as necessary, with approval.

44. The third-party provider or cloud service provider must provide TO Live the capability of performing regular access reviews at least annually.

**Access Control and Credential Management Principles and Process Guidelines**

45. Access controls and credential management must be enforced in alignment with security frameworks (e.g., PAN-Canadian Trust Framework (PCTF) and the frameworks governed by the National Institute of Standards and Technology (NIST)). This will provide assurance that TO Live's login and authentication processes are secure and will protect its technology and information assets from unauthorized access.

**Enforcement of Policy**

46. Prior to using any TO Live infrastructure, IT assets and/or information, authorized users should request a clarification through their Manager, Supervisor, or the Director of Information Technology if they have any concerns regarding compliance with this policy.

47. Security breaches or incidents, suspected or confirmed account compromises, must be immediately reported to the Director of Information Technology.

48. Non-compliance can lead up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with due 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 should request a clarification through their supervisor if they have any concerns regarding compliance with this policy.

49. TO Live shall ensure compliance with this policy across the organization, with assistance of the Director of Information Technology, by providing direction on individual responsibilities and the specific procedures to be followed. Department VP's and Directors should have a reporting cadence with the Director of Information Technology to confirm that their department employees, contractors, service providers, and vendors are compliant.