ATTACHMENT 2

TO Live

FINANCE POLICY

Title	Effective Date	Policy Number
Signing Authority	January 2018 March 31, 2022 February 27 2025 March 24, 2026	301

This policy outlines the required two signatories for contracts that commit TO Live to a commitment above $499.99. Any contract below $499.99, or as outlined in the Financial Delegation of Authority for Purchasing Policy #303 for the minimal threshold requirement for a purchase order, may be signed by the Department Head and the Director or Manager.

Contracts must be expressly for the business purposes of TO Live.

1. Payments must be signed by two of the following:

   *Any one of:
   - President & CEO
   - VP of Finance & Administration

   *The above noted officers will not have processing access to the accounting system.

   And one of the following:
   - Director of Finance
   - Controller
   - Senior Accountant

2. Contracts for At Risk Presentations presented by TO Live must be signed by two of the following:

   - President & CEO
   - VP, Executive Producer
   - VP of Finance & Administration

   The above noted officers must ensure that the terms and conditions of the above noted contracts adhere to the terms of Finance Policy #305 – “At-Risk Presentations” and exceptions must be presented to the Board of Directors for approval.

3. Collective agreements and Memorandum of Understandings must be signed by two of the following,

   One of:
   - President & CEO

And **after approval of the Board of Directors**, one of the following:

- VP of Operations
- VP of Finance & Administration
- VP, Executive Producer
- VP of Human Resources & Organizational Culture

The above noted officers must ensure that the collective agreement terms and conditions adhere to the threshold terms provided by the Board of Directors for bargaining. All collective agreements must be approved by the Board of Directors of TO Live before signature.

4. Agreements for rental of the facilities for an attraction must be signed by two of the following:

   One of:
   - VP, Executive Producer
   - Director of Programming

   And one of:
   - President & CEO
   - VP of Finance & Administration
   - Director of Finance

   An attraction rental is defined as a ticketed public event.

   The above noted officers must ensure that the terms and conditions of the above noted contracts adhere to the terms of Rental Policy #302 – “Rental contracts” and exceptions must be presented to the Board of Directors of TO Live for approval.

5. Agreements for Communities & Outreach events, including artists and instructor contracts must be signed by two of the following

   One of:
   - President & CEO
   - VP, Executive Producer
   - VP of Finance and Administration

   And one of:
   - VP, Executive Producer
   - Director of Programming
   - Director of Communities & Outreach
   - Director of Finance

6. Agreements for rental of the facilities for a corporate or private event must be signed by two of the following:

   One of:
   - Director of Corporate & Private Events
   - VP, Executive Producer
   - Director of Rental Events

   And one of**:**
   - President & CEO
   - VP of Finance & Administration
   - Director of Finance

   A corporate or private rental is defined as a non-ticketed, non-public event.

7. Sponsorship contracts, Grants and Gift Agreements must be signed by two of the following:

   One of:
   - President & CEO
   - VP of Finance & Administration

   And one of:
   - VP of Philanthropy & Sponsorship
   - Director of Philanthropy & Sponsorship

8. All other commitments, including but not limited to any legal, financial, professional and/or consulting service, either jointly shared by organizations other than TO Live or where TO Live is participating in the re-imbursement of costs engaged by one of the joint participants, must be signed by two of the following:

   One of:
   - President & CEO
   - VP of Finance & Administration

   And one of:
   - VP of Operations
   - VP, Executive Producer
   - VP of Marketing & Communications
   - VP of Philanthropy & Sponsorship
   - VP of Human Resources & Organizational Culture

   All commitments with a value of $300,000 or greater in aggregate must be approved in advance by the Board of Directors of TO Live.

9. This policy is to remain in effect until otherwise directed or modified by the Board of Directors of TO Live.

10. This policy should be considered in conjunction with policy #303 – Financial Delegation of Authority for Purchasing.

TO Live

FINANCE POLICY

Title	Effective Date	Policy Number
Financial Delegation of Authority for Purchasing	May 2019 March 2022 February 2025 March 2026	303

PURCHASING POLICIES

1. Prior to the actual purchase of any goods or services of a value above $499.99, an approved purchase order (PO) is required. At least one quote must accompany all POs and all amounts should be stated net of HST.

2. All POs must have at least two (2) approvals as outlined below. Please note that the requester and the approver can be the same person.

3. A PO is considered approved after it has been “issued”. This is only possible once it has reached the final approval stage.

4. The Accounts Payable Clerk handles the processing of all invoices under $499.99, reaching out to the purchasing department when further information is needed (i.e. when a GL code has not been provided).

5. The "splitting" of a PO so as to keep each invoice under an approval level is not permitted.

6. **At-risk performance contracts** include a commitment to a marketing budget. This **attraction marketing budget** is the PO and cost cap for attraction marketing expenses as issued by the VP, Executive Producer and/or VP of Marketing & Communications. See policy #305 – At Risk Presentations.

7. **The VP of Marketing & Communications** or designate **MUST** ensure that the placement of advertising/marketing costs engaged on behalf of **rental clients** has been secured by confirmed deposits before a commitment to suppliers is made. If needed, a schedule of expected advertising/marketing deposits can be given to accounting, and accounting will monitor the payment terms.

8. When more than one department is sharing the cost of purchases, the PO and invoice should be approved by all participating departmental authorities.

9. Completed POs shall be authorized by the appropriate authority as outlined below prior to ordering goods and/or services for daily operations. Authorization for purchasing advertising expenses on rental and risk attractions is covered in points 6 & 7 of this policy. The authority levels for all other purchases are:

Level	Requester	Approver	Final Approver	
$499.99 - $1,999.99	Any staff member up to Manager	Any staff member up to Manager	Manager or Senior Manager	
$2,000 - $4,999.99	Any staff member up to Manager	Manager or Senior Manager	Director	
$5,000 - $7,499.99	Any staff member up to Director	Director	Departmental VP	
$7,500 - $24,999.99	Any staff member up to Departmental VP	Departmental VP	VP Finance	
$25,000 - $99,999.99	Any staff member up to VP of Finance	VP Finance	President & CEO	
Over $100,000 (Capital only)				Approval of the Board of Directors of TO Live
Over $300,000 (Operating only)				Approval of the Board of Directors of TO Live

10. In order to determine if a PO is required and at what level of signing authority is required, the value of the PO will be calculated taking into consideration the aggregate costs, including multiple year arrangements and all applicable taxes, if applicable.

11. No Manager/Director/VP shall approve the purchase of an item intended for the personal use of an employee of TO Live. No Manager/Director/VP shall authorize the use of company property for the personal use of an employee (even where there is an intention to reimburse TO Live). Employees allocated a digital device (smart phone, etc.) shall reimburse TO Live for any unreasonable personal roaming charges incurred through use of the digital device immediately upon receipt of a request from accounts payable. Each employee travelling outside Ontario shall make themselves aware of the rules for minimizing roaming charges on digital devices.

12. This policy should not be confused with reimbursements for legitimate business expenses covered in Finance Policy #314.

13. <u>Paying independent contractors by invoice – unincorporated entities</u>

    It is each VP's responsibility, in cooperation with the VP of Finance & Administration, to determine if an independent contractor is an incorporated entity or not. Invoices payable to unincorporated entities (persons in most cases) fall under the following rules:

Commitments to pay under $2,000 per annum:
Have the independent contractor sign off on the independent contractor form provided by Accounts Payable. Use of this form assumes a casual minimum cost use of the independent contractor. The form sets out the independent contractor relationship and the contractor's responsibility for treating their invoiced income as self-employed.

Commitments to pay over $2,000 per annum:
Either a personal services contract is prepared and approved by the VP of Finance & Administration prior to approval and payment of any invoices for services rendered **OR** all payments will be treated as subject to T4A filing rules.

No commitments should be entered into until an agreement with the VP of Finance & Administration has been concluded.

14. Policy Relating to Lobbying in the Purchasing Process

TO Live is committed to the highest standards of integrity with respect to the purchase of goods and services and management of the process by which goods and services are acquired. This section of the policy relating to lobbying in the purchasing process applies to the purchase of all goods and services and to all vendors and suppliers, with the exception of risk productions and rental attractions and events.

Unsolicited communications by vendors and suppliers with TO Live staff, officials or Board members are subject to the provisions of Chapter 140, Lobbying, of the Municipal Code of the City of Toronto. Unless an exemption under Chapter 140 applies, vendors and suppliers must register with the City's lobbyist registry prior to communicating with TO Live. Definitions of "communication" and "lobby" are included Section 140-1 of Chapter 140, which also outlines registration requirements, exemptions, a code of conduct, and potential penalties.

The requirements to register as set out in the City of Toronto Municipal Code; Chapter 140 shall apply to all TO Live procurements except those dealing with the acquisition of risk productions and rental attractions and events.

Any questions relating to the applicability of Chapter 140 of the Municipal Code should be directed to the Office of the City of Toronto's Lobbyist Registrar.

15. Blackout Period

During all formal or structured procurement processes initiated by TO Live, an official point of contact will be named by TO Live to respond to communications and inquiries in relation to a call or other purchasing process. This point of contact will be in effect from the time of issuance up to and including the announcement of the purchasing award or approval. During this time, there is a blackout period when vendors/suppliers, any representatives employed by them, or any unpaid

representatives acting on their behalf, are strictly prohibited from communicating verbally or in writing (including by electronic means) with TO Live Board members, officials or any staff other than the official point of contact. All communications with respect to a call or purchasing process must be made to the official point of contact, and any vendors/suppliers found to be in breach of this policy will be subject to disqualification from the current and any future calls or procurement processes at the sole discretion of the Board.

16. All senior staff of TO Live shall ensure that this policy is provided to all vendors and suppliers.

17. All Capital Purchases not approved as part of the annual budget process must be approved by the President & CEO and the VP of Finance & Administration or Director of Finance, and if valued over $100,000, approved by the Board of Directors of TO Live.

18. Special exceptions for emergency situations of values over $100,000 must be approved by the VP of Finance & Administration or the President & CEO and the Chair of the Board and then presented to the Board.

PURCHASING PROCEDURES

Please refer to the Purchase Order Procedure Manual (for the EBMS purchasing module) and Policy #301 Signing Authority.

TO Live

FINANCE POLICY

Title	Effective Date	Policy Number
At-Risk Presentations	April 2017 March 31, 2022 February 27 2025 March 24, 2026	305

Annual Budget

Board approval is required for each individual Attraction where artist fees, estimated marketing expenditures, and any other non-recoverable costs in aggregate, ***less*** any co-venture sharing, exceed $300,000 Canadian dollars.

As part of the annual budget process, the Board of Directors of TO Live requires that the President & CEO along with the VP, Executive Producer bring forward the "At-Risk Budget" for Board approval. During this process, the following information must be provided to the Board:

- the break-even business model
- the budget target net revenue used in the annual budget
- the marketing rationale
- any alternate contractual arrangements for Treasury, if known.

For any At-Risk Presentation not approved as part of the annual budgeting process, including identifying alternate Treasury arrangements (if applicable), the Board of Directors of TO Live requires that it be brought forward for Board approval for each individual Attraction as per the same terms noted above.

Management will provide an update on all At-Risk presentations as part of the quarterly financial report.

Definitions:

At-Risk Presentation: A presentation of any attraction by TO Live in which TO Live management contractually takes a risk position on the probability that associated net treasured receipts will fund the attraction's net costs.

Attraction: A performing arts event (artist, company, festival, installation etc.)

Treasury (of box office receipts): All tickets sold by TO Live box office or its designated agents are to be treasured by TO Live through its authorized ticket agency until the attraction has been presented before box office receipts are released at settlement.

TO Live

CYBERSECURITY POLICY

Title	Effective Date	Policy Number
Personal Passwords	September 20 2023 February 27 2025 March 24, 2026	502

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 fourteen (14) passwords.
  - Cannot contain your account or full name.
  - Cannot contain anything related to your job function.
  - Cannot contain words – tolerance 5.
  - Cannot be found in compromised password list.
  - Cannot be found in TO Live dictionary.

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.

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
2025-01-28	1.2	Annual Review	David McCracken
2025-01-28	1.2	Updated Password Requirements	David McCracken
2026-01-02	1.3	Update Previous Passwords to 14 in section 1 to be baseline compliant.	David McCracken
2026-02-09	1.4	Added points 5 + 7 for clarity that this policy applies to admin and service accounts and changes should only be made via secure channels	David McCracken

TO Live

CYBERSECURITY POLICY

Title	Effective Date	Policy Number
Mobile Device Management	September 20 2023 February 27 2025 March 24, 2026	504

This Mobile Device 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 means that the user and TO Live must take to ensure the security and integrity of the device by verifying that the necessary components have been installed with the latest version; and
- the approach to managing the types of software and applications installed on each device and ensuring all activity performed on the device does not violate TO Live's policies and standards; and
- the defined requirements to effectively manage access through authentication and password requirements; and
- the required actions to take when a device that has access to TO Live resources is compromised or lost.

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.

Provision of Mobile Devices and Responsibilities

1. TO Live reserves the right to determine which staff members will be provided with a company owned mobile device for usage in connection with TO Live's business.
2. Where TO Live provides a mobile device to any staff member, TO Live retains the sole discretion with respect to the continued provision of the mobile device for work purposes.
3. Information stored on mobile devices, whether TO Live owned or not, is the property of TO Live. TO Live may, at any time without notice, access, review, copy, transfer or delete any data stored on any mobile device, whether company owned, or a personal Bring Your Own Device (BYOD), including but not limited to e-mails and data downloaded from the internet.
4. Mobile devices accessing TO Live data must be updated regularly by owner/holder to run the latest approved operating system (OS) version and security patches.
5. Mobile devices accessing TO Live data, including BYOD, are centrally managed by the Information Technology Department Mobile Device Management (MDM) platform to ensure devices are actively being monitored, updated, and secured.
6. TO Live's MDM platform enforces the use of security settings such as PIN use, screen timeouts, and minimum operating system requirements.
7. Software and/or application installations on mobile devices may be restricted by TO Live. The MDM may be used to enforce the removal and/or restrict the types of installations on mobile devices to ensure that only authorized software and/or applications are deployed and are configured, in a manner that does not compromise the integrity of the device and the associated data. If the MDM solution cannot automatically remove the software, the user may be directed to remove the software manually before being able to access TO Live resources.
8. Compatible Endpoint Security software that is approved by the Information Technology Department is required to be installed on mobile devices. Users must not tamper or interfere with the Endpoint Security software installed onto mobile devices.
9. The activity performed on mobile devices may 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 cybersecurity incident.
10. All discovered or suspected data breaches that occur on any mobile device used to access TO Live data must be immediately reported to the Director of Information Technology.
11. The MDM solution may be used to implement a remote wipe, remote disablement, or device locking commands on mobile devices that have access to TO Live data. These processes will be initiated in the event that the device is lost or stolen, an

employee has reached the end of their employment, or other situations that pose a security threat to TO Live. While efforts to provide prior notice to end users will be taken, TO Live retains the right to carry out these actions as deemed necessary to protect TO Live data.

12. Tampering with or altering company-approved operating systems (e.g., auto screen lock timer, jail-breaking, unauthorized installation of beta releases or non-approved third-party operating system builds) on mobile devices accessing TO Live data is strictly prohibited.

13. In case of a regulatory or legal requirement to examine a mobile device, upon request, the employee must surrender the device to the Directory of Information Technology for a reasonable time to allow forensic imaging for as long as may be required by a court of competent jurisdiction.

14. Mobile devices must adhere to the authentication requirements dictated by the Director of Information Technology as well as TO Live's MDM platform.

15. Mobile devices must comply and 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, and the minimum OS that should be employed. Mobile devices that cannot comply and support secure communication will be blocked from accessing any TO Live data.

16. Data stored on devices must not be synchronized with external systems that are not approved by TO Live.

17. Users are responsible for ensuring the physical security of mobile devices to guard against loss or theft.

18. In the event of loss or theft of devices that contain any TO Live data, users should immediately report it to the Director of Information Technology to ensure services and access from the device are disabled pending recovery or replacement of the mobile device.

Mobile Device Usage

All staff provided with mobile devices for usage in connection with business of TO Live are required to adhere to the following:

19. To limit the use of the mobile device to either responding to or otherwise addressing any matters related to work during scheduled business hours; or hours beyond regular scheduled hours, if approved by your manager.

20. Significant, additional, out of plan "roaming" charges are incurred when using mobile devices outside of Canada. Staff are required to get authorization from their manager before taking their mobile device outside of Canada. When

approved by your manager, the use of mobile devices outside of Canada is to be restricted to business use only. Due care and diligence to minimize additional "roaming" voice and data charges is expected. Roaming packages are available for mobile device use outside of Canada. The Information Technology department should be consulted at least one week prior to a mobile device being used outside of Canada so adequate roaming packages can be considered, purchased, and applied to the existing data plan.

21. All business charges for a mobile device will be allocated to the department in which the mobile device user works.

22. TO Live retains the right to bill individual staff users for additional charges outside the mobile device plan arising from excessive usage unrelated to business.

23. Employees are expected to use mobile devices in a manner consistent with the fact that any data stored on or transmitted via the device may become public.

24. Staff are strictly prohibited from utilizing mobile devices at any time when you are the driver of a moving vehicle. This is contrary to the law. Any employees found in contravention of this law will be solely responsible for liabilities, claims, and damages arising out of the contravention of any law. Furthermore, the staff member will be at risk of having the mobile device privilege withdrawn.

25. Employees are expected to use mobile devices in such a way as to ensure that nothing stored on or transmitted via the device will expose TO Live or its employees to any legal liability or result in public embarrassment to TO Live or its employees.

26. Use of mobile devices are also subject, at a minimum, to the following TO Live Policies:

    - Code of Conduct – Policy 200
    - Remote Work – Policy 201
    - Confidentiality – Policy 205
    - Personal Passwords – Policy 502
    - Credential Management – Policy 505

Enforcement of Policy

27. 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.

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

29. 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.

30. 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.

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	Added clarity for BYOD	David McCracken
2024-02-18	1.1	Added section for MDM PIN, screen, and minimum OS. 6	David McCracken
2025-01-28	1.2	Annual Review	David McCracken
2025-01-28	1.2	Change anti-malware/anti-virus to Endpoint Security in section 8	David McCracken
2026-01-02	1.3	Updated to remove specific TLS version in section 15	David McCracken

TO Live
CYBERSECURITY POLICY

Title	Effective Date	Policy Number
Artificial Intelligence	March 24, 2026	511

This Artificial Intelligence (AI) Policy establishes the objectives, requirements, and standards that all employees, contractors, vendors and service providers must follow to protect the confidentiality, integrity, and availability of TO Live's technology and information assets. This policy applies to all current and future artificial intelligence technologies used within TO Live, regardless of how they are delivered, integrated, or accessed.

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, with respect to AI, including:

a) Establishing an approach to managing AI applications, platforms, software, and technology; and
b) Ensuring AI use complies with TO Live's existing policies and standards; and
c) Outlining best practices and critical thinking requirements for AI use; and
d) Defining required actions when AI use or data is suspected to be compromised or outside acceptable TO Live standards.

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.

Application of Policy

1. AI applications, platforms, software, and technology are not to be used for any commercial or business purpose not related to the business of TO Live.
2. All information created, downloaded, entered, generated, or stored using AI applications, platforms, software, or technology is the property of TO Live. TO Live may at any time without notice access, review, copy, transfer or delete any applications, materials, programs, and/or data stored in AI applications, platforms, software, or technology.
3. Employees must use AI in a manner that does not expose TO Live or its employees to any legal liability or reputational harm.
4. Employees must use AI with the understanding that any material created, downloaded, entered, generated, stored, or transmitted through AI may become public.
5. Use of AI platforms and technology are also subject, at a minimum, to the following TO Live Policies:
    - Policy 105 - Fraud and Other Irregularities
    - Policy 200 - Code of Conduct
    - Policy 201 - Remote Work
    - Policy 205 - Confidentiality
    - Policy 501 - Security and Awareness Training
    - Policy 503 - Personal Computers

Oversight & Accountability

6. This policy will be reviewed annually.
7. AI projects that have significant public impact will undergo an internal ethics and sustainability assessment by the Director of Information Technology and Senior Management at a minimum.
8. Staff and collaborators using AI must complete TO Live assigned AI training before using any approved and licensed AI applications, platforms, software, or technology.

General Use Principles

9. Personal data (audiences, staff, artists) will not be processed using AI applications, platforms, software, or technology without consent and compliance with privacy regulations.

10. Sensitive or confidential personal data must not be entered into any AI application, platform, software, or technology. This includes any information that can be used to personally identify an individual such as a home address, driver's license, health card number, or social insurance number.

11. Data created, downloaded, entered, generated, stored or transmitted using AI applications, platforms, software, or technology must not contain content that violates applicable laws, breaches confidentiality obligations, infringes intellectual property rights, or expose TO Live to legal, regulatory, or reputational harm.

12. TO Live is committed to compliance with Human Rights legislation. AI-generated or AI-assisted content that discriminates or comments negatively on individuals based on protected grounds (including race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, age, marital status, family status, disability, or the receipt of public assistance) is strictly prohibited.

13. AI must not be used to copy or transmit any of TO Live's applications, data, documents, software, or other information in contravention of copyright laws or intellectual property rights.

14. AI must not be used in the transmission or storage of any defamatory, derogatory, obscene, offensive, pornographic, abusive, sexist, racist, threatening, harassing, or false messages, or messages that disclose personal information without authorization.

15. Employees must not use AI to access or attempt to access or view or download material pornographic, obscene, racist, or otherwise inappropriate material whose content is inconsistent with TO Live's obligation to ensure compliance with the Human Rights Code.

16. Employees must immediately notify the Director of Information Technology if they encounter AI material generated or other material that contravenes this policy.

17. All data created, downloaded, entered, generated or stored by employees in any AI application, platform, software, technology or otherwise remains the property of TO Live. Unauthorized removal of data from any AI application, platform, software, technology or otherwise is strictly prohibited.

18. The use of employee-owned devices with TO Live approved and licensed AI applications, platforms, software, or technology is strictly prohibited. This includes, but is not limited to, computers, USB drives and any removable storage media. Only TO Live issued and authorized devices may be used to access TO Live AI systems.

19. AI applications, platforms, software, or technology used by TO Live must be licensed and approved by the Director of Information Technology. All licenses are registered

and regulated by the Information Technology Department. As a matter of policy, TO Live does not permit the use of, or the installation of unlicensed or personally owned software on its owned computers. If in doubt, please consult the Director of Information Technology.

20. Requests for AI applications, platforms, software, or technology for business use must be submitted to the IT Help Desk – ithelpdesk@tolive.com. The Information Technology department will review all requests for legitimacy and proper licensing.

21. Acquisition of AI platforms and/or software applications is subject to TO Live Policy 303 - Purchasing Policies & Procedures.

Critical Thinking

22. Recognize that AI systems are tools designed to assist, not replace, human judgment.

23. Be aware of the limitations of AI, including potential biases, inaccuracies, and lack of contextual understanding. AI-generated content may contain inaccurate, misleading, or fabricated information and must be independently verified before being relied upon.

24. Avoid over-reliance on AI outputs without human validation, especially in high-stakes or sensitive contexts.

25. Question the accuracy, relevance, and appropriateness of AI-generated content.

26. Cross-check AI recommendations or decisions with trusted sources or expert input.

27. Document decisions made with AI assistance, including rationale and supporting evidence.

28. Understand that ultimate responsibility for decisions made with AI support rests with the human operator.

Ethical & Inclusive Use

29. AI tools must be selected and applied in ways that avoid bias, stereotyping, or discrimination.

Enforcement of Policy

30. 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.

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

32. 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 legislation. Authorized users should request a clarification through their supervisor if they have any concerns regarding compliance with this policy.

33. 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 Vice Presidents 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.