Acceptable Use of Technology at the Bereavement Authority of Ontario

Contents

Contents 1
Scope 1
Purpose 2
Background 2
Policy 3
Procedures 5
Revision Log 6

Scope

This policy applies to all BAO employees, contractors, consultants, Board Members, Officers, and approved users, as well as all BAO information systems, devices, and technology assets. This includes, but is not limited to:

- Desktop and laptop computers
- Tablets and mobile devices
- Servers and storage media (physical and cloud)
- Physical documents
- Corporate software and applications
- Internal networks (e-mail, SharePoint, etc.)
- External networks (internet, telephone systems, voicemail, photocopiers, etc.)

Purpose

The objective of this policy is to define and inform employees and approved users of information security best practices and standards regarding the use of the Bereavement Authority of Ontario's (BAO) information systems, devices, and technology resources. This ensures company-owned equipment, sensitive data, and corporate assets are properly protected, and BAO operations remain secure, reliable, and compliant.

Background

The Bereavement Authority of Ontario (BAO) relies on secure, reliable, and well-managed information systems to conduct its regulatory responsibilities and support day-to-day operations. As technology continues to evolve, so do the risks associated with improper use, data breaches, and cyber threats.

To protect the integrity of BAO operations, maintain public trust, and ensure compliance with legislative, contractual, and security obligations, it is essential that all employees and approved users understand and adhere to established standards for the use of BAO technology and information systems.

This policy outlines the expectations, responsibilities, and acceptable use standards for BAO-issued equipment, networks, software, and digital information. It provides a

framework to safeguard corporate assets, ensure operational continuity, and support a secure and productive work environment.

Definitions

Artificial Intelligence: Information technology capable of performing tasks that would ordinarily require human intelligence, such as analyzing information, recognizing patterns, learning from data, generating content, or making predictions and recommendations.

Authorized User: an employee, contractor, or approved individual who has been granted permission to access the organization's information systems, data, or devices.

Confidential Information: any data that is not intended for public release and must be protected from unauthorized access, including personal information, internal documents, and sensitive operational material.

Device: any hardware used to access organizational systems or data, including desktops, laptops, mobile phones, tablets, and peripherals.

Personal Use: non-business activities performed on organizational systems or devices that are allowed only within approved limits.

System: any technological platform, application, network, or service owned, managed, or provided by the organization.

Policy

It is the responsibility of all BAO personnel to take reasonable care in the use of BAO technology and systems to ensure their long-term functionality and integrity. Employees and users are accountable for all activity conducted under their assigned usernames. Misuse, negligence, or deliberate abuse of BAO resources may result in disciplinary action, up to and including dismissal.

The BAO provides technology resources to enhance productivity and support business objectives. All systems must be used in a responsible, ethical, and lawful manner, in compliance with BAO policies, contracts, and applicable legislation. Misuse of technology can negatively impact the BAO, its employees, the bereavement sector, or the public.

Acceptable Use

- Employees and approved users are encouraged to use BAO technology to support legitimate business purposes, including:

- Communicating with colleagues, business partners, licensees, or consumers within the scope of assigned responsibilities.
- Acquiring, processing, or sharing information necessary to perform job duties.
- Supporting organizational operations, administration, and productivity.

- The following uses are strictly prohibited:
  - Activities that are illegal, fraudulent, malicious, or violate BAO policies and procedures.
  - Accessing, sharing, storing, or distributing content that is indecent, discriminatory, offensive, or harmful to BAO operations or reputation.
- Limited personal use of BAO technology is permitted, provided it:
  - Does not interfere with job performance.
  - Does not negatively impact network or system performance.
  - Does not limit access to shared technology resources.
  - Does not misrepresent or harm the reputation of the BAO.
- All use of BAO systems may be monitored for system analysis, IT planning, compliance, security, and investigation purposes.

Data Security

- Employees and approved users must protect BAO data and information systems from unauthorized access, loss, or disclosure. The BAO provides each user with cloud-based storage space for files and documents. All BAO work must be stored on approved BAO environments to ensure that files are properly backed up and not accessible from local hard drives in the event a device is lost or stolen.
- The following data security practices must be followed:
  - Only BAO approved software and technology may be used or installed on BAO computers or devices.
  - Users may not disable, circumvent, or tamper with any BAO security controls, nor install unauthorized security tools or hardware.
  - Any BAO data stored on mobile storage devices such as USB drives or smartphones must be password protected and encrypted.

    - BAO data must not be stored on personal storage media or personal cloud services such as Google Drive, OneDrive (on a personal email), or Dropbox.
    - Mobile devices must not be left unattended in public places.
- Employees must always be aware of the sensitivity of data stored on BAO equipment and ensure that privacy, confidentiality, and corporate security are maintained.

Physical Security

- BAO-issued equipment must be protected from loss, theft, and damage at all times.
    - When travelling for business, equipment must remain in the employee's possession whenever possible.
    - If equipment must be left in a vehicle, the vehicle must be locked, and the equipment must be placed out of sight before reaching the destination.
- Employees must take appropriate precautions in high-risk locations such as conference centres, where electronic equipment is frequently targeted.
- If a BAO device is stolen:
    - Local authorities must be notified immediately.
    - The BAO Senior Manager, Information Technology must be contacted at ari.finkelstein@thebao.ca.
    - IT Management will disable device access and, where available, remotely erase the contents of the device.
- Employees are not permitted to take BAO equipment on vacation or personal travel without express approval from their manager.

Roaming

- If there is any potential for roaming charges on a BAO device, employees must contact IT Management before travelling. IT will determine the most appropriate and cost-effective action such as enabling a roaming package or recommending the purchase of a local SIM card.
- Employees are encouraged to turn off mobile data when using Wi-Fi to prevent accidental roaming and unnecessary costs.

Surrender of BAO Assets

- All BAO issued equipment, identification cards, access credentials, and other assets must be returned to the organization when:
    - Employment or a contract ends.
    - An employee begins a Leave of Absence.
    - An employee begins maternity or paternity leave.
- All returns must be coordinated with IT Management or the employee's supervisor to ensure proper deactivation and inventory tracking.

Related Documents

- **Acceptable Use of Artificial Intelligence:** IT P&P 26 Acceptable Use of Artificial Intelligence.docx

Revision Log

Revision	Date Revised	Short Description of Revision
1	November 17, 2025	Initial draft
2	November 18, 2025	Revisions for clarity