

CITY OF KETCHUM RESOLUTION 25-003

A RESOLUTION OF CITY COUNCIL OF THE CITY OF KETCHUM, IDAHO, TO APPROVE AND ADOPT INFORMATION TECHNOLOGIES (IT) POLICIES AND PROCEDURES.

WHEREAS, IT policies and procedures ensure the security, efficiency, and reliability of technology infrastructure.

WHEREAS, as a municipality serving the public, we strive to perform technology data functions to the highest level of service.

WHEREAS, we adhere to best practices for system maintenance, data backup, and cybersecurity to protect organizational assets and sensitive information.

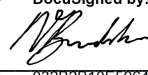
WHEREAS, as a municipality, we align IT strategies with best practices in mind. We use guidance from Idaho Counties Risk Management Program (ICRMP) as they provide recommendations for many policies and procedures in Idaho.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF KETCHUM IDAHO:

Approval and adoption of Information Technology (IT) Policies and Procedures.

This resolution will be in full force and effect upon this 6th day of January, 2025.


CITY OF KETCHUM, IDAHO

DocuSigned by:


032B2B10E596435...
Neil Bradshaw

Mayor

ATTEST:
Signed by:



7FAF0B9BC7D8434...
Trent Donat
City Clerk

Signed by:





CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager
direct: 208.806.7010 | office: 208.726.3841
tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340
ketchumidaho.org

City of Ketchum | IT Policies and Procedures

January 6, 2025

1. IT Policies and Procedures Statement

IT policies and procedures ensure the security, efficiency, and reliability of technology infrastructure. As a municipality serving the public, we strive to perform technology data functions to the highest level of service. We adhere to best practices for system maintenance, data backup, and cybersecurity to protect organizational assets and sensitive information.

2. Municipality IT Policies and Procedures Scope Summary

As a municipality, we align IT strategies with best practices in mind. We use guidance from Idaho Counties Risk Management Program (ICRMP) as they provide recommendations for many policies and procedures in Idaho. We also use National Institute of Standards and Technology (NIST) as part of defining the Cyber Policy framework.

3. Municipality IT Procedure for Acceptable Use

3.1. Purpose

The Acceptable Use Policy outlines the appropriate and responsible use of municipality IT resources to ensure security and efficiency. This policy has each employee read and sign to understand and maintain adherence to Technology Policies and Standards.

3.2. Scope

This policy applies to all employees, contractors, and third-party users accessing municipality IT systems and data.

3.3. General Use

- IT resources must be used for legitimate business purposes only.
- Personal use of municipality IT resources should be minimal and not interfere with job responsibilities.
- Technology User Account Password Standards:
 - Incorporate multi-factor, password less, or equivalent secure login methods.
 - Require passwords to be changed at the latest of 90 days.
 - Minimum of 10 characters in length.
 - Cannot contain the user's account name.
 - Must contain upper- and lower-case characters.
 - Must contain at least one non-alphanumeric symbol.
 - Base 10 digits (0 through 9)
 - Cannot be a repeat of the last 6 passwords - standards where hardware and operating systems limitation allow it.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager

direct: 208.806.7010 | office: 208.726.3841

tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340

ketchumidaho.org

- All authenticated sessions will be secured by a screen saver after 15 minutes of inactivity. Exceptions to this policy based on business needs.
- All personnel will perform their work under his/her own credentials. Sharing of credentials is not permitted.
- Employees will not share their credentials with one another.
- All personnel will be held responsible for all transactions made using their credentials.
- Electronic “caching” of credentials is discouraged.
- Systems shall regard seven consecutive failed login attempts as a trigger to lock the account for 30 minutes.

3.4. Prohibited Activities

- Unauthorized access to systems, networks, or data.
- Distribution of malicious software or engaging in activities that compromise network security.
- Use of IT resources for illegal activities, including copyright infringement or harassment.
- All data is the property of the municipality and shall not be taken in any form for personal use.

3.5 Email and Communications Tools

- Professional language and conduct are required in all communications.
- Confidential information must not be shared through unsecure channels.
- All email is backed up and becomes part of the historical record based on the Records Retention Policy Schedule for the City of Ketchum and can be accessed by submitting a Public Records request.

3.6 Internet Usage

- Access to inappropriate or non-business-related websites is prohibited.
- Downloading unauthorized software or large files without approval is not allowed.

4. System and Network Security

4.1. Municipality IT Data Disaster and Recovery

IT Systems and Security Procedures are designed to protect the integrity, confidentiality, and availability of technology infrastructure and data. Data is backed up regularly, and disaster recovery plans are in place to ensure business continuity. Ongoing training and adherence to industry best practices are essential to maintaining a secure and efficient IT environment.

- Municipality Data is backed up in a 3-2-1 best practice. The 3-2-1 backup strategy states that you should have 3 copies of data (production data and 2 backup copies) on two different media (disk and other) with one copy off-site for disaster recovery.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager

direct: 208.806.7010 | office: 208.726.3841

tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340

ketchumidaho.org

- A Read-Only, unchangeable (immutable) set protects from ransomware and is also part of the backup strategy.
- Recovery Time Objective (RTO) is calculated and balanced for efficiency. This relates to how quickly data recovery can occur from a Data Breach and or malware/ransomware attack.
- Recovery Point Objective (RPO) is calculated and balanced for efficiency. This relates to what timeframe last data backup can be recovered from in the case of a Data Breach and or malware/ransomware attack.

4.2. Data Breach and Communications Policy

NIST Cybersecurity Framework plan of action steps ongoing.

- Ongoing Governance to identify risk, expectations, and policy
- Identify current cybersecurity risks and trends
- Protect and apply safeguards to reduce cybersecurity risk
- Detect and analyze possible cybersecurity attacks and compromises
- Respond to action regarding an incident
- Recover assets and operations post impact
- Improve processes to better serve the municipality

4.3 Cybersecurity Incident Action Plan

1. Immediate Response: Upon detecting a data breach, the Business Manager must be alerted within 24 hours. A decision of impact will be determined to formulate next steps. If the incident has compromised systems and data in a critical fashion, an Incident Response Team (IRT) will be assembled.
 - The Business Manager will be notified and become the point person for all aspects of the incident.
 - The Community Engagement Manager will manage all internal and public communications.
 - ICRMP Cyber Insurance team will be contacted and activated within 72 hours. An IRT will assemble conforming to need and type of event.
 - An outside forensics team (remote and onsite) will be deployed as part of ICRMP
 - Internal resources will be used to gather information, contain the breach, and protect assets.
2. Assessment and Containment: The IRT will assess the breach's scope and contain the incident to prevent further data loss. It is important to isolate and preserve data breach evidence.
3. Internal Communication: Key stakeholders, including senior management and IT, must be informed promptly about the breach by the Communications Team.
4. Regulatory Notification: Regulatory bodies will be notified within the timeframe required by law, typically within 72 hours.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager

direct: 208.806.7010 | office: 208.726.3841

tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340

ketchumidaho.org

5. Customer Notification: Affected customers will be informed about the breach, potential risks, and protective measures they can take within 72 hours.
6. Public Disclosure: If the breach is substantial, a public statement will be issued to maintain transparency and trust via the Communications Team.
7. Ongoing Updates: Regular updates will be provided to stakeholders and customers on the investigation and remediation efforts.
8. Strategically restore systems and data and monitor integrity of data and processes.
9. Review and Improvement: Post-incident, a thorough review will be conducted to improve security measures and prevent future breaches.

4.4 AI Usage Guidelines

- Do not submit any sensitive or private information to a Generative AI platform you would not want available to the public.
- Create a Generative AI system account just for City usage.
- Carefully review, verify, and fact check via multiple sources the content generated by Generative AI.
- Cite or reference when you use Generative AI within your documents and communications.
- Opt out of data collection whenever possible.

4.5 Internet of Things (IoT)

- All IoT devices deployed on a City Wi-Fi network should be certified fully compliant with the latest 802.11 standard. Certification of compliance may be requested.
- All IoT devices deployed should support the 5GHz band.
- All IoT devices should provide an easily accessible MAC address prior to device onboarding.
- Default passwords must be changed or disabled.
- Universal Plug and Plan (UPnP) must be disabled.
- Remote management should be disabled unless an exception is granted by City IT Security.
- Firmware must be kept up to date on a pre-approved schedule.
- Encryption and certificates should be used wherever applicable.
- Devices should be physically secured in a manner that prevents tampering.
- Control Access: Use firewalls and network segmentation to only allow trusted connections and limit incoming/outgoing traffic to IoT devices.
- Inventory All Devices: Maintain a frequently updated inventory of all IoT devices used.

5. Municipality-Owned Devices Procedures Statement

Procedures for municipality-owned devices ensure the secure and efficient use of all hardware provided to employees. Devices must be used primarily for business purposes, with minimal personal use permitted. Security measures, including password protection, encryption, and regular software updates, must be followed to protect municipality data. Employees are



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager
direct: 208.806.7010 | office: 208.726.3841
tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340
ketchumidaho.org

responsible for the care and proper use of these devices and must report any loss, theft, or damage immediately to IT support.

- The use of Artificial Intelligence (AI) constructs is allowed but must go through an approval process.
- The Use of Internet of Things (IoT) is allowed but must go through an approval process. A dedicated and segmented network does exist to allow these devices to operate off the main network.

6. Monitoring and Compliance

IT activities are subject to monitoring to ensure compliance with this policy. Violations of the Acceptable Use Policy may result in disciplinary action, up to and including termination.

7. Review and Updates

This policy will be reviewed periodically and updated as necessary to address new threats and changes in technology.

The Goal for Responsible Technology

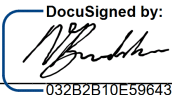
IT Policies and Procedures encompass end user guidance, system maintenance, data management, and cybersecurity to safeguard and optimize the technology infrastructure. They include regular updates, audits, and compliance checks to ensure operational integrity and adherence to ICRMP standards. Additionally, staff training and support are integral to procedures promoting efficient and secure use of IT resources.

8. Acknowledgment

The IT Policies and Procedures Policy has been approved and adopted. This guide will assist in the direction of all technology strategy and planning for City of Ketchum.

Date:
1/9/2025

City of Ketchum

By:  _____
032B2B10E596435...

Title:
mayor



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager

direct: 208.806.7010 | office: 208.726.3841

tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340

ketchumidaho.org

City of Ketchum Acceptable Use Policy | Technology

January 6, 2025

1. Introduction

This Technology Acceptable Use Policy ("Policy") outlines the acceptable use of technology resources provided by City of Ketchum ("Municipality"). The purpose of this policy is to ensure the responsible and secure use of technology assets, including but not limited to, computer systems, networks, internet access, and electronic devices, by all employees, contractors, and third-party users.

2. Scope

This policy applies to all individuals who have access to Municipality's technology resources, including employees, contractors, consultants, temporary workers, and other users. The policy covers all forms of technology, whether owned by the Municipality or provided by a third party.

3. Acceptable Use

3.1. Authorized Users:

Only authorized individuals are permitted to use the Municipality's technology resources. Authorized users include employees, contractors, and other individuals approved by the Municipality.

3.2. Data Security:

Users must take all necessary precautions to protect sensitive and confidential information. This includes using strong passwords, not sharing login credentials, and encrypting sensitive data when applicable.

- A strong user account and password policy should enforce the use of complex passwords, including a mix of uppercase and lowercase letters, numbers, and symbols, while also requiring regular password updates to enhance security.
- The Municipality asks that you select a password or passphrase that is complex and secure.
- Changing your password every 90 days is the expectation for applications.
- Refrain from re-using passwords or using a single password for multiple accounts.
- Additionally, implementing secondary authentication methods such as an email code, SMS text, or preferably an authentication App adds an extra layer of protection by requiring users to verify their identity through multiple means.
- The detailed list of requirements can be found in the IT Policies and Procedures document. The IT support team will assist with the implementation of these initiatives.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager

direct: 208.806.7010 | office: 208.726.3841

tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340

ketchumidaho.org

3.3. Prohibited Activities:

The following activities are strictly prohibited:

- a) Unauthorized access to or use of computer systems, networks, or data.
- b) Using USB drives is prohibited unless a valid business case merits their use.
- c) Distribution or installation of malware, viruses, or any malicious software.
- d) Intentionally attempting to bypass security measures or hacking into systems.
- e) Engaging in any form of cyberbullying or harassment.
- f) Using personal computers and devices to access sensitive city information.
- g) Downloading and use of any Municipality data outside of employment scope.
- h) Intentionally deleting organizational data with intent to cause harm.

3.4. Internet Usage:

Internet usage is allowed for work-related purposes. The Municipality provides Public Wi-Fi access and users must abide by the Terms of the Agreement to use this amenity. Excessive personal use is discouraged. Users are prohibited from accessing inappropriate or offensive websites.

Employees are expected to use the organization's internet resources responsibly and in accordance with applicable laws and policies. Unauthorized access, distribution of inappropriate content, and any activities that compromise network security are strictly prohibited.

4. System and Network Security

The end user policy for system and network security mandates adherence to strong password practices, regular software updates, and the prohibition of unauthorized software installations. Additionally, users are required to report any suspicious activities or security incidents promptly to the designated IT support channels.

4.1. System Integrity:

Users must not attempt to compromise the integrity or availability of computer systems, networks, or data. Our end user policy underscores the paramount importance of maintaining system integrity to safeguard against unauthorized access, data breaches, and potential disruptions. Users are expected to adhere to stringent security measures, promptly report any suspicious activities, and actively participate in maintaining a resilient and secure computing environment.

4.2. Data Backup Policy:

All Municipality data is backed up regularly to ensure business continuity in the event of a disaster or system failure. Employees are required to ensure that Municipality owned data is located within folders and locations that backup systems can accurately backup up data.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager
direct: 208.806.7010 | office: 208.726.3841
tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340
ketchumidaho.org

4.3. Malicious Software:

All users are required to have updated antivirus software on their devices. If any suspicious activity is detected, users must report it immediately to the Business Manager and/or the IT Support team.

4.3. Data Breach Procedures:

In the event of a suspected cyber incident or data breach, the municipality will promptly identify and employ a third-party consultant to contain the breach, notify affected parties and relevant authorities in a timely fashion, and conduct a thorough investigation to prevent future incidents. All communications regarding the breach will be transparent, accurate, and timely. We will provide support to affected individuals, including guidance on protecting personal information and mitigating potential harm. Continuous improvements to our security measures and training programs will be implemented to enhance our data protection protocols.

- If you see or suspect a technology incident has occurred, immediately contact your supervisor or Department Manager who will contact the Business Manager. It is imperative to keep all communications (internal and external) occurring through the Community Engagement Director.
- Initial Point of Contact: Supervisor or Department Manager who will contact the Business Manager. If the Business Manager is not available, then notification goes to the City Administrator.
- All PR Communications shall be coordinated by: Community Engagement Manager
- Cyber incidents are reported to Municipality Cyber Insurance Agent: ICRMP

5. Municipality-Owned Devices

End users are required to use Municipality devices responsibly and exclusively for work-related purposes to ensure data security and confidentiality. Any unauthorized use, including the installation of non-approved software or accessing restricted content, is strictly prohibited and may result in disciplinary action.

5.1. Device Usage:

- Municipality-owned devices are intended for business purposes. Personal use should be kept to a minimum.
- The use of Municipality devices such as printers for personal use should be kept to a minimum. Speak with your manager about any special projects.

5.2. Software Installation:

Users are not allowed to install unauthorized software on Municipality-owned devices. Submit an IT Support ticket to set up a request and guidance for additional software needs.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager

direct: 208.806.7010 | office: 208.726.3841

tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340

ketchumidaho.org

5.3. Internet of Things (IoT):

IoT is a growing segment of useful devices performing specific functions. All IoT devices need to be approved before deployment. Maintain an up-to-date list of all IoT devices. Place IoT devices on a separate network segment and use strong encryption for data transmission to protect the main corporate network. Ensure regular software and firmware updates for all IoT devices to protect against vulnerabilities. Provide ongoing training on IoT security best practices and regularly review and update the security policy to address new threats and advancements in technology.

5.4. Use of Artificial Intelligence (AI):

Generative AI has the potential to deliver significant benefits by increasing efficiency and productivity. Simultaneously, current Generative AI implementations may carry risks, including inaccurate or unreliable outputs (“hallucinations”), biased or inappropriate outputs, security vulnerabilities, intellectual property (IP) and privacy concerns, and legal uncertainties.

Use of Approved Generative AI. Examples would be ChatGPT, CoPilot, Vasa2, etc.

1. Each new use-case of Generative AI should be subject to an approval process.
2. Use of safety features. Each user should be required to enable all available safety features.

The use of Generative AI platforms may be permitted for the purpose of increasing personal administrative productivity. Any such use should fully take into consideration the user:

1. Do not submit any sensitive or private information to a Generative AI platform you would not want available to the public.
2. Create a Generative AI system account just for City usage.
3. Carefully review, verify, and fact check via multiple sources the content generated by Generative AI.
4. Cite or reference when you use Generative AI within your documents and communications.
5. Opt out of data collection whenever possible.

6. Monitoring and Enforcement

6.1. Monitoring:

The Municipality reserves the right to monitor technology resources to ensure compliance with this policy.



CITY OF KETCHUM

Trent Donat | City Clerk & Business Manager
direct: 208.806.7010 | office: 208.726.3841
tdonat@ketchumidaho.org

P.O. Box 2315, 191 5th Street West, Ketchum, ID 83340
ketchumidaho.org

The IT Support team does use several monitoring systems to troubleshoot and proactively inspect use and system behavior.

6.2. Enforcement:

Violations of this policy may result in disciplinary action, including termination of employment or legal action.

6.3. User Training and Professional Development:

Regular IT training ensures employees are aware of security best practices, can recognize potential threats, and know how to respond appropriately to security incidents. All users are enrolled in a training program offered by ICRMP that defines technology security awareness and best practices. It is expected that all employees will actively pursue educational opportunities to apply the safest approaches to the use of technology and protecting assets.

7. Review and Updates

7.1. Policy Review:

This policy will be reviewed periodically to ensure its relevance and effectiveness.

7.2. Updates:

The Municipality reserves the right to update this policy as needed. Users will be notified of any changes.

8. Acknowledgment

By using City of Ketchum's technology resources, all users acknowledge that they have read, understood, and agree to comply with this Technology Acceptable Use Policy.

Employee Name: _____

Date: _____

Signature: _____

Title: _____