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: _____