Acceptable Use Policy

Contents

Purpose

The purpose of this policy is to meet the enterprise business objectives and outline the acceptable use of computer equipment and other electronic devices at Ambient Enterprises Holdco LLC. These rules are in place to protect the employees and Ambient Enterprises Holdco LLC. Inappropriate use exposes Ambient Enterprises Holdco LLC to cyber risks including virus attacks, ransomware, compromise of network systems and services, data breach, along with potential legal or reputational issues.

Scope

This policy applies to all Ambient Enterprises Holdco LLC employees, subsidiary employees, contractors, consultants, temporary workers, third parties, and other workers who have access to IT assets of Ambient Enterprises Holdco LLC and may be bound by contractual agreements. This policy and guidelines shall be made available to, communicated to, and understood by all users of Ambient Enterprises Holdco LLC IT assets.

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Ambient Enterprises Holdco LLC business or interact with internal networks and business systems, whether owned or leased by Ambient Enterprises Holdco LLC, the employee, or a third party. All employees, contractors, consultants, temporary staff, and other workers at Ambient Enterprises Holdco LLC and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Ambient Enterprises Holdco LLC policies and standards, and laws and regulations.

Roles & Responsibilities

The roles and responsibilities for executing this policy include the following:

Chief Information Security Officer or designated personnel: The security manager or designated personnel shall be responsible for the implementation and

dissemination of the acceptable use policy and ensuring that all users are aware of the policy and agree to it.

Information security team: The information security team shall be responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy and to set controls that identify misuse.

IT department: The IT department shall be responsible for building, configuring, operating, and maintaining the corporate email facilities (including anti-spam, anti-malware, and other email security controls) in accordance with this policy.

IT Help/Service Desk: The IT Help/Service Desk shall be responsible for assisting users with secure use of email facilities, acting as a focal point for reporting email security incidents, and assisting users with other general IT issues.

Internal audit: Internal audit operated by an independent firm, or any Ambient Enterprises Holdco LLC employee or subsidiary employee authorized to run an audit, are authorized to assess compliance with this policy and other corporate policies at any time.

Definitions

AI: Artificial Intelligence

Ambient Enterprises Holdco LLC / Company / Corporate: Refers to employees of Ambient Enterprises Holdco LLC and all subsidiaries' employees operating under names or trademarks approved during merger and acquisition.

Authorized Use: Authorized use of Ambient systems is defined as access by an active, provisioned user account, from a Ambient-managed and compliant endpoint, authenticating via MFA, performing functions consistent with the user's assigned role, in support of legitimate business operations.

Incident: An event that, as assessed by staff, threatens the confidentiality, integrity, or availability of information systems or the information on which they are stored, processed, or transmitted; or that constitutes a violation of security policies, security procedures, or acceptable use policies.

Information Asset: Any Ambient Enterprises Holdco LLC data in any form that is used while executing business. This includes, but is not limited to, corporate, customer and third-party data.

Information Systems: Any Ambient Enterprises Holdco LLC equipment, applications or systems used to manage, process, or store Ambient Enterprises Holdco LLC data. This includes, but is not limited to, information systems managed by third parties.

IT assets: Includes, but is not limited to, hardware assets, software assets, cloud services, network assets, utilities (including air conditioners and power), closed-circuit television (CCTV), physical security systems and devices, and telecommunications services.

Laws and Regulations: Includes local, city, state, federal, and international laws and regulations for citizenship, residency, and travel. Questions regarding applicability should be directed at Ambient Enterprises Holdco LLC's General Counsel.

ML: Machine Learning

User(s): All employees, contractors, and third parties who have access to IT assets of Ambient Enterprises Holdco LLC and may be bound by contractual agreements.

General Use and Ownership

Acceptable Use: Corporate IT resources and communication systems are intended primarily for business purposes. Personal use of these resources is permitted only as allowed under applicable law. Additionally, employees should not use personal computer devices for business purposes unless specifically authorized by the Security Manager or designated personnel. Approval for personal use shall be sent to human resources and stored in the individual's personnel files. Users accessing company data through mobile devices that are personally owned shall not save corporate data on personal devices outside of the application it is intended. Nor shall any employee use personal cloud services such as OneDrive Personal, Dropbox, Google Drive, or any other personally owned cloud services to conduct business or store company data. If users have corporate applications on a personal mobile device, the mobile device is required to have biometrics and/or a minimum PIN length of six digits activated, in addition to auto-lock features being enabled.

Personal Use: Employees are responsible for reasonableness of personal use on any corporate electronic device and do so at their own risk of exposure of personal data and risk of disciplinary action up to and including termination of employment. Individual departments or subsidiaries may not create less stringent policies than corporate policies unless written approval is received from the Chief Information Security Officer and Chief Information Officer. In the absence of such policies, employees should be guided by corporate policies on personal use. If there is any uncertainty, employees should consult their human resources representative, supervisor, or manager.

Privacy and Ownership: While the security administration of Ambient Enterprises Holdco LLC desires to provide a reasonable level of privacy, users should be aware that the data they create and/or store on corporate systems remains the property of Ambient Enterprises Holdco LLC. Because of the need to protect IT assets, management cannot guarantee the confidentiality of personal information stored on any IT asset belonging to Ambient Enterprises Holdco LLC. All content on Corporate IT resources, including but not limited to messages, files, data, documents, facsimiles, telephone conversations, social media posts, and other forms of communication, is considered property of the Company. Consequently, a user should have no expectation of privacy regarding any information transmitted, received, printed from, stored, or recorded on Corporate systems. Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their human resources representative, supervisor, or manager.

Security and Proprietary Information

Electronic Devices: All mobile and computing devices that connect to the internal network must comply with the corporate access policies. If there is any uncertainty, employees should consult their human resources representative, supervisor, or manager.

Proprietary Information: Ambient Enterprises Holdco LLC proprietary information stored on electronic and computing devices — whether owned or leased by Ambient Enterprises Holdco LLC, the employee, or a third party — remains the sole property of Ambient Enterprises Holdco LLC. The individual accessing Ambient

Enterprises Holdco LLC data must ensure through legal or technical means that proprietary information is protected, must promptly report the theft, loss, or unauthorized disclosure of proprietary information, and may access, use, or share such information only to the extent it is authorized and necessary to fulfill assigned job duties.

Monitoring and Access: The Company reserves the right to monitor, intercept, and review all data transmitted, received, or downloaded over its IT resources and communication systems, in line with applicable laws. This monitoring may occur periodically without prior notice. For IT system security and network maintenance purposes, only authorized individuals within Ambient Enterprises Holdco LLC shall monitor equipment, systems, and network traffic at any time. Authorized individuals include the Chief Information Security Officer, IT Infrastructure Manager, Chief Information Officer, and the managed service provider. All other individuals must gain approval from the Chief Information Officer and Chief Information Security Officer, who will consult and/or notify HR and Legal. Ambient Enterprises Holdco LLC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Data Security and Confidentiality: Activities that may degrade the performance of the Company's IT resources, restrict access to authorized personnel, or circumvent security measures are strictly prohibited. Employees are also barred from downloading, installing, or running unauthorized programs or utilities.

Passwords: Passwords must be maintained in strict confidentiality and should never be visibly posted or stored in accessible locations. Employees are responsible for ensuring that printed documents containing confidential information are immediately removed from printers and fax machines. All third-party purchases of software or cloud services must be approved by the Chief Information Security Officer and Chief Information Officer. Access to the software or services should be single sign-on and multi-factor authentication (MFA) unless the approved software does not allow the capability. System-level and user-level passwords must comply with the corporate password policies. Providing access to another individual, either deliberately or through failure to secure their access, is prohibited. Shared passwords or shared multi-factor authentication are strictly prohibited.

Licensing: At no time shall a corporate employee circumvent licensing terms of service when purchasing software or cloud services by sharing software or login credentials to reduce cost or for any other justification. Unlawful use of any third-party software license is grounds for discipline up to and including termination of employment.

Security Awareness Training: As part of your responsibility towards maintaining the integrity and security of the Company's IT infrastructure, you are required to complete the Company-provided cybersecurity awareness training courses within 30 days of them being assigned.

Device Security: All corporate electronic devices must be secured with a password-protected lock screen with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended. Users shall not change or manipulate any system to increase auto-locking of corporate systems. Users are responsible for reporting permissible access that appears to be more than they should have. Users may face discipline up to and including termination if access logs show a user accessed unauthorized data without reporting the issue to the IT Infrastructure Manager, Chief Information Security Officer, or Chief Information Officer.

Social Media and Information Sharing Services: Postings by employees from a corporate email address to newsgroups or other online platforms should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of any corporate name or trademark, unless the posting is being performed as a job responsibility.

Email: Employees must use extreme caution when opening email attachments or clicking links received from unknown senders or unexpected email from known users, which may contain malware.

Computer Security and Copying of Software

Software programs purchased and provided by Ambient Enterprises are to be used only for creating, researching, and processing materials for Company use. By using Company hardware, software, and networking systems you assume personal responsibility for their use and agree to comply with this policy and other

applicable Company policies, as well as laws and regulations. Violation of software licensing, whether personal licensing on corporate devices, company licensing, or lack of license availability, may result in disciplinary action up to and including termination of employment.

All software acquired for or on behalf of the Company, or developed by Company employees or contract personnel on behalf of the Company, is and will be deemed Company property. It is the policy of the Company to respect all computer software rights and to adhere to the terms of all software licenses to which the Company is a party.

You may not illegally duplicate any licensed software or related documentation. Unauthorized duplication of software may subject you and/or the Company to both civil and criminal penalties under the United States Copyright Act.

You may not duplicate, copy, or give software to any outsiders including clients, contractors, customers, and others. You may use software on local area networks or on multiple machines only in accordance with applicable license agreements entered into by the Company.

Mobile Devices

Mobile Device Usage (Both Personal and Business): If you drive a vehicle during your employment, you may not use any cell phone, mobile device, or other communication device while driving unless the device is equipped or configured with a "hands-free" listening/speaking option, and you in fact utilize that hands-free device. It is the Company employee's responsibility to understand allowed usage of mobile devices in accordance with laws and regulations. Company employees shall follow whichever is strictest between Company policies and applicable laws or regulations.

Employer-Provided Cell Phones / Mobile Devices: Ambient Enterprises Holdco LLC may issue certain employees a Company cell phone or mobile device for work-related communications and/or operations. Personal use of employer-provided devices is permitted; however, such personal use should not exceed the plan allowance. When the device is used for personal reasons and the activity results in additional cost to the Company, the employee is responsible for that usage cost,

including all applicable taxes unless prohibited by law. The Company owns and remains entitled to all cell phones and mobile devices issued to employees. At the time of employment termination, all such equipment must be returned to the Company in operable condition. Violation of this policy may result in legal action.

Personal Cell Phone / Mobile Device Use: While Ambient Enterprises permits employees to bring personal cell phones and other mobile devices (e.g., tablets, laptops) into the workplace, employees must not allow such devices to interfere with job duties or impact workplace safety and health. Use of personal devices at work can be distracting and should primarily occur during non-working time such as breaks and meal periods. Employees may be required to install company-approved software or security tools on their personal devices if used for work purposes. By doing so, employees agree to comply with all applicable Company policies regarding data security and usage. Violation of this policy may result in disciplinary action up to and including termination of employment.

Prohibited Uses

The following activities are prohibited:

- Harassing, threatening, or abusing others.
- Using personal or non-approved Artificial Intelligence services.
- Intentionally degrading the performance of Company information resources.
- Committing the organization to a third party — for example through purchase or sales contracts, job offers, or price quotations — without explicit authorization by management.
- Purposefully circumventing Company security measures.
- Accessing, creating, storing, or transmitting material which may be deemed offensive, threatening, obscene, illegal, or intentionally false or inaccurate.
- Engaging in any activity that is illegal under any law or regulation while utilizing Company-owned resources.
- Unauthorized disclosure of private and/or confidential information.
- Using Company resources to circulate unauthorized solicitations or advertisements for non-organizational purposes, including religious, political, or not-for-profit entities.

- Providing unauthorized third parties, including family and friends, access to Company IT information, assets, resources, or facilities.
- Misrepresenting, obscuring, suppressing, or replacing another user's identity in transmitted or stored messages.

Ethical Guidelines

Employees should be aware that if they identify or suspect fraud, corruption, theft, or any unethical business practices in the workplace, they should feel able and prepared to share their concerns within the Company. This policy enables all employees to raise concerns without fear of discrimination or victimization because of whistleblowing. Violations of ethical guidelines leave employees at risk of disciplinary action up to and including termination of employment. Ethical guidelines include:

Personal Relationships at Work and Conflicts of Interest: Any employee involved in a close personal relationship with a colleague, contractor, client, customer, or supplier must not allow that relationship to influence their conduct at work. It is your responsibility to identify when it is appropriate to inform your manager of any relationship or association that has the potential to create a conflict of interest. Personal relationships do not supersede an employee's responsibility to protect Company data.

Bribery, Corruption & Facilitation Payment: The Company will not tolerate any form of bribery by, or of, its employees, agents, or consultants or any person or body acting on its behalf. Employees or associated persons who report instances of bribery in good faith will be supported by the Company. The Company will terminate the contracts of any associated persons found to have breached this policy. Employees and associated persons conducting business outside the US may be at greater risk of exposure to bribery or unethical conduct and owe a duty to the Company to be extra vigilant when conducting international business.

Compliance with Laws: Local, regional, state, federal, and international laws are to be followed regarding conducting business, using technology resources, and protecting company and user data. Employees should act in the best interests of the Company following any required regulatory laws or compliance requirements within the area they are conducting business, whether in-person or remotely. If

there are any questions or lack of understanding, the Company legal department should be contacted.

High-Risk Use of AI Systems

The intent of this policy section is to provide general guidance on the use of AI at Ambient Enterprises so that Ambient Enterprises can leverage AI as a tool while ensuring it continues to meet legal obligations and act in an ethical manner. Users should only use Company-provided AI tools. Submitting or providing any Company data to an AI tool that is unapproved or personally owned is strictly prohibited. Any tool (hardware, software, cloud service, or mobile application) being purchased for use within the Company must be approved by the IT Infrastructure Manager, Chief Information Security Officer, and Chief Information Officer. Please reach out to helpdesk@ambient-enterprises.com to initiate the request process. Any features of AI and/or ML must be disclosed at the time of request prior to purchase.

The use of AI at Ambient Enterprises should never compromise its core values or introduce undue risk to the organization; rather, it should be focused on improving business efficiencies and enhancing Ambient Enterprises' ability to fulfill its mission. Ambient Enterprises is a global organization with entities and staff globally; accordingly, this policy provides overarching guidance based on global standards. Representatives should be cognizant that the use of AI in some countries may not be permitted in others.

- AI systems must not share or gain ownership of data inputted.
- AI should not introduce new risks to the organization.
- AI should be used to improve business efficiencies.
- If you travel or live internationally, be aware of local regulations regarding AI and data being transmitted or stored.
- When using AI, users should have subject-matter expertise in the area for which AI is being used.
- AI cannot itself be used for validation of final accuracy; it may only be used as support to the end result.

Use Standards & Use Approval

The process for using unapproved or new resources involves submitting a formal request with justification to your manager. If approved, the formal request should then be sent to helpdesk@ambient-enterprises.com, CC'ing the approving manager. Managers in leadership roles will bypass the pre-approval step and send requests directly to helpdesk@ambient-enterprises.com. The request is evaluated based on factors such as business need, security, compatibility, cost, and compliance, then reviewed by the Approval Authority. All steps are documented. Approved resources are installed by IT personnel. The Approved List is reviewed and updated as needed.

Exceptions

Any exceptions to this policy or its associated requirements must be formally documented, reviewed, and approved in advance by the Chief Information Security Officer. Approved exceptions shall include a defined business justification, compensating controls where applicable, and an expiration or review date to ensure continued oversight.

Document Handling

This document will be reviewed, approved, and distributed in accordance with the Policy Management process and procedure as defined by Ambient Enterprises. All subsequent changes will be logged under the "Revision History" section of this document. This document must be reviewed and updated at least once per year. Material changes are communicated within 30 days.

Violations & Penalties

Violations of this policy must be immediately reported to any involved managers and the IT Department. Non-compliance with any subsection of this Acceptable Use Policy may result in disciplinary action. Consequences may range from mandatory refresher training and written warnings to termination of employment or contractual obligations. Individuals could be subject to legal consequences under

applicable laws if violations involve illegal activities. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the infraction of policy, law, or regulation.