# Wireless LAN User Acceptable Use Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of the Wireless Local Area Network (WLAN) user acceptable use policy is ensure secure and appropriate use of [Company Name’s] WLAN services.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions i.e. those people, elements or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all [Company Name] WLAN and network services as well any and all users of [Company Name] WLAN and network services.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. **Wireless Local Area Network (WLAN).** This is defined as a wireless network contained to a specific area containing access points which provide internet connectivity to computers equipped with wireless capabilities.
2. **Access Point.** This is defined as a device which creates a point of wireless internet connectivity in which total bandwidth is shared between users of the network.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. [Company Name] will provide employees with a personal, nontransferable, and nonexclusive account-enabling access to the Internet via [Company Name] wireless internet access point.
2. Installation, operation, and maintenance of all [Company Name] WLAN service shall be the responsibility of [Company Name’s] IT Department.
* WLAN users will not deploy access points that extend the coverage of [Company Name’s] WLAN service unless otherwise authorized by [role/department].
1. [Company Name] (and its affiliates and their respective partners, directors, limited liability company managers, officers, employees, and agents) shall have no liability or responsibility for, any direct, indirect, incidental, or consequential damages suffered by users in connection with their use of or inability to use the WLAN service, including, but not limited to, damages from loss of data resulting from delays, non-delivery, mis-delivery or service interruptions, or due to inadvertent release or disclosure of information sent by the user even if the same is caused by [Company Name’s] own negligence.
2. [Company Name] disclaims to the full extent permitted by applicable law and responsibility for (and under no circumstances shall [Company Name] be liable for) any conduct content, goods, data, and services available on or through the internet or the WLAN service.
3. In no event shall [Company Name] aggregate liability exceed the amount paid by users to [Company Name] for the use of the WLAN service, if any. Use of any information or data obtained via the WLAN service and the internet is at the users own risk, and [Company Name] (and its affiliates and its and their respective partners, directors, limited liability company managers, officers, employees, and agents) disclaims any responsibility for the completeness or accuracy of any such information or data.
4. From time to time the WLAN Service may be inaccessible or inoperable for any reason, including, without limitation: (i) equipment malfunctions; (ii) periodic maintenance procedures or repairs which [Company Name] may undertake from time to time; or (iii) causes beyond the control of [Company Name] or which are not reasonably foreseeable by [Company Name].
5. Users shall be solely responsible for providing, maintaining, and ensuring compatibility with the WLAN Service, all telecommunications and computer hardware, software, telecommunications access charges, lines or connections, or other equipment and services required to access and use the Service. Furthermore, users are solely responsible for the security, confidentiality, and integrity of all messages and content they receive, transmit through, or store on through or via the WLAN Service.
6. There are significant security, privacy, and confidentiality risks inherent in accessing or transmitting information through the Internet, whether the connection to the Internet is facilitated through wired or wireless technology. These security issues range from interception of transmissions, loss of data, or the introduction of viruses or other programs that can damage user computers or networks. [Company Name] shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused in connection with user access to or transmission of information through the Internet.
7. Users are solely responsible for any authorized or unauthorized access to their account by any person. Users will bear all responsibility for the confidentiality of their account, where applicable, and all use or charges incurred from use of the WLAN Service with their password.
8. Users will not engage in any inappropriate use of the WLAN Service. Inappropriate use includes, but is not limited to:
	* Transmitting any information or data, in any form, that violates any local, state, federal, or applicable international law or regulation, or that is harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, and invasive of another’s privacy, hateful, or otherwise objectionable.
	* Violating or infringing of any copyright, trademark, patent, or other statutory or common law proprietary rights of others.
	* Sending unsolicited mass email messages (spam).
	* Engaging in any activity or device in an effort to disguise the origin of any transmission.
	* Transmitting any information or data that contains any computer virus, or any material designed to interrupt, destroy, or limit the functionality of any computer hardware or software.
	* Engaging in any activity in the nature of hacking or port scanning.
	* Engaging in any activity that is or may be harmful to minors.
	* Using the WLAN Service in furtherance of any fraudulent activity.
	* Engaging in any activity that is in the nature of a denial of service attack.
	* Engaging in forgery or impersonation.
	* Using the WLAN Service to collect personal data or attempt to collect personal information about third parties without their knowledge or consent.
	* Reselling access to the WLAN Service without [Company Name’s] express written authorization.
	* Engaging in any activity that adversely affects the ability of other people or systems to use the WLAN Service or the Internet.
	* Engaging in any other activity deemed by [Company Name] to be in conflict with the spirit or the intent of this Agreement.
9. The WLAN Services are intended for periodic active use of email, instant messaging, browsing the World Wide Web, and other typical end-user activities. High-volume data transfers, especially sustained high-volume data transfers, are prohibited. Hosting a web server, IRC server, or any other server is prohibited.
10. [Company Name] reserves the right to disconnect users from the Internet and deny access to the WLAN Service at any time, issue warnings (written or verbal), bill users for administrative costs and/or reactivation charges, and bring legal action to enjoin violations and/or to collect damages, if any, caused by violations.
* [Company Name] reserves the right, in its sole discretion and without notice, at any time and for any reason, to: (i) remove or disable access to all or any portion of the WLAN Service; (ii) suspend User’s access to or use of the WLAN Service; (iii) reduce the bandwidth available to User; and (iv) terminate this Agreement.
1. [Company Name] (and its affiliates and its and their respective partners, directors, limited liability company managers, officers, employees and agents) shall have no liability with respect to any claims, losses, or expenses by any party arising out of or relating to: (i) user breach of this Policy; (ii) user use of the WLAN Service, including any data or work transmitted or received by users; and/or (iii) any inappropriate use of the WLAN Service, including, without limitation, any statement, data, or content made or republished by users which is prohibited by this Policy.
2. [Company Name] reserves the right to modify this Policy at any time, effective upon posting of the modified Policy. Therefore, you are urged to review this Policy frequently.
3. The fee (if any) charged by [Company Name] for your use of this WLAN Service is paid solely for the privilege of accessing this Service. Other websites you visit may charge additional fees.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.