**Instant Messaging Usage & Security 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.

**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.

Instant Messaging (IM) is currently being used by [Company Name] as a form of real-time communication with individuals inside the organization. IM technology is meant for the purpose of enhancing employee productivity while conducting [Company Name] business. However, IM carries some security risks that must be addressed.

The use of IM at [Company Name] is a privilege and its abuse or misuse will not be tolerated. It is the responsibility of the IT department to manage and monitor IM usage and ensure that this policy is adhered to. It is the responsibility of the user to exercise sound judgment and common sense while using IM to fulfill his or her job duties.

**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 IM use at [Company Name] headquarters, district offices, and remote locations. This policy applies to all [Company Name] employees, including full time, part time, contractors, interns, consultants, suppliers, and other third parties.

**Definitions**

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

**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. **Supported IM Solution:** [Company Name] has selected [name IM solution] as its soleprovider of corporate IM services. Non-sanctioned IM services could affect network security, so the corporate firewall has been configured to block them. Free IM services commonly used within the consumer market are NOT approved or supported by the IT department.
2. **Acceptable Use:** IM services are to be used for business communications and for the purpose offulfilling job duties, in accordance with corporate goals and objectives. Use of IM communications in this manner between [Company Name] employees and project teams is permitted and encouraged. It is expected that all employees will communicate professionally with colleagues, keeping in mind that foul language and slang terms are not allowed. [Note: If IT allows external IM communications with business partners or clients, these can be referred to here. However, this should only be done with added security features provided by IM security vendors.]
3. **Confidentiality:** The transmission of sensitive corporate information through IM for businesspurposes is not permitted. Truly sensitive communications should be conducted through encrypted e-mail or in-person meetings. Employees are prohibited from sending client lists, personal information, credit card information, trade secrets, and other proprietary information through the corporate IM service. In addition, it is prohibited to discuss legal advice or questions through IM with corporate lawyers, as this can violate the attorney-client privilege.
4. **File Sharing:** Though many IM services support the transmission of files, this feature has beenblocked for IM at [Company Name]. [Note: Although Info-Tech recommends the banning of file sharing altogether, if advanced network-based security controls are in place, this section can be modified to include that file sharing is permitted and that all files will be automatically scanned for viruses and monitored by IT.]
5. **Personal Use:** Limited personal use of corporate IM services to communicate internally withcolleagues at [Company Name] regarding non-work-related matters is permitted during designated work breaks and lunch hours only. Even during allotted personal IM usage periods, employees may not use the service for unsolicited mass mailings, non-[Company Name] commercial activity, operation of a privately owned business, solicitation of funds, dissemination of political causes, or promotion of religious/personal beliefs to others.
6. **Compliance:** IM use at [Company Name] will comply with, all [Company Name] policies, all[Company Name] contracts and all applicable laws.

1. **Privacy:** IM conversations and messages created on the corporate IM service and transmittedthrough corporate systems will be considered the property of [Company Name]. [Company Name] reserves the right to monitor, inspect, copy, review, store, and audit IM usage and messages generated by or for the enterprise. [Company Name] is also obligated to disclose IM messages and conversations when ordered to do so by auditors, courts, and law enforcement, with or without the employee’s consent. Given these factors, employees do not have a reasonable expectation of privacy when using corporate IM services.
2. **Record Retention:** Instant messages are considered business records and are thus subject to[Company Name’s] existing policies and procedures regarding business record retention, storage, and deletion.
3. **Unacceptable Use:** Individual IM use must not interfere with others’ use of [Company Name’s]IM services. The following activities are deemed inappropriate uses of [Company Name] systems and services and are therefore prohibited:

Use of IM for illegal or unlawful purposes, including copyright infringement, obscenity,

libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

Use of IM in any way that violates [Company Name’s] policies, rules, or administrative orders, including, but not limited to, [list any applicable code of conduct policies, etc.].



Viewing, copying, altering, or deleting IM accounts or files belonging to [Company Name] or another individual without authorized permission.



Sharing IM account passwords with another person, or attempting to obtain another

person’s IM account password. IM accounts are to be used by the registered user only. Allowing a non-registered user to use an account is not permitted.

**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. Temporary or permanent revocation of IM access;

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.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of** | **Author** | **Rationale** |
|  | **Change** |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |