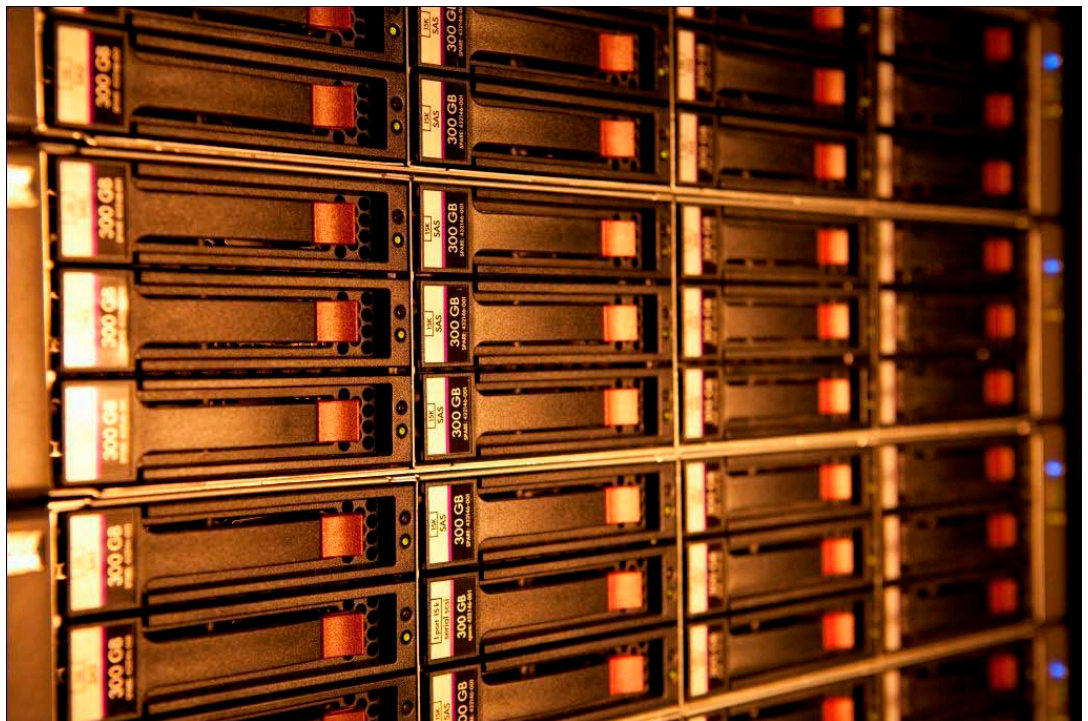


Acceptable Use Policy



POL 0014

Revision A



Table of Contents

Document Control and Revision History..... 3

1. Summary..... 4

2. Terms and Definitions..... 5

3. Prohibited Activities..... 6

4. Security 7

5. Password Protection..... 7

6. Rights and Remedies 7

7. Reference Documents..... 9

Document Control and Revision History

Rev Level	DCO Number	Brief Description of Change	Effective Date MM/DD/YY
A	10001	Initial Draft	05/05/10
A	10002	Approved by Randy Gibson, Process and Service Mgr	05/10/10
A	10003	Added to Prohibited Activities – Jennifer Morrison	10/22/10
A	10004	Changed Block Removal – Jennifer Morrison	10/25/10
A	10005	Approved by Jennifer Morrison, ITSM	10/25/10
A	10006	Branding Template	11/02/10
A	10007	Add Terenine Service Mark	11/02/10
A	10008	Approved Ron Beaver, President	11/03/10

1. Summary

This document describes the Terenine Acceptable Use Policy. This policy is designed to help ensure the security, privacy and integrity of Terenine's Clients and their data. The Acceptable Use Policy details what activities by our Clients and their users are prohibited via our services, as well as described actions Terenine may take in response to a violation of this policy. This policy applies to all aspects of Terenine's services.

This policy is based on the principles stated by the Terenine Security Policy.

These rules rely on the following essential principles:

- Usage of Information Systems is, by principle, reserved for professional use.
- Access to Information Systems must be conducted with the access codes handed out by the Administrators.
- Internet connection must be achieved with User authentication by accessing secure channels through access points documented in the Information Systems function.
- All software must be appropriately licensed and software installation must be done exclusively by the Information Systems function.
- Confidential information must be encrypted.
- Transmitting information over the Internet must be watched closely.

The Client is responsible for ensuring that all persons accessing or using the services comply with the Acceptable Use Policy.

Actual, indirect or attempted violations of this Acceptable Use Policy by a Terenine Client or that Client's Users will be considered violations of the policy.

If a Client becomes aware of any violations of this Terenine Acceptable Use Policy, Terenine requests immediate notification to Director of Service Operations. Terenine will notify its Clients of any complaints received by us regarding alleged violations by that Client's Users; each Client shall provide a contact person for such communications. Terenine and the Client agree to promptly investigate all violations, alleged violations and complaints; all necessary actions will be taken to remedy violations of this policy.

2. Terms and Definitions

- **FTP Server:** A server connected to the Internet which is used to transfer or download files using standard File Transfer Protocol (FTP).
- **Phishing:** Attempting to acquire information by masquerading as a trustworthy entity.
- **Spam, Junk Mail, and Unsolicited Commercial E-Mail (UCE):** Transmission of substantially similar unsolicited E-mail messages to more than one recipient which includes E-mail with forged headings, false contact information or sent via compromised mail server relays.
- **Unsolicited Message:** A message that is sent to a recipient who has not requested the message or posted in violation of a newsgroup or Web site rules.

3. Prohibited Activities

Users agree to use the service only for lawful purposes. Terenine's Clients and their Users are prohibited from utilizing Terenine network or services to perform or participate in any illegal, unethical or harmful activities or practices including, but not limited to:

- **Spamming:** Aimed at sites or via E-mail, i.e., sending or posting messages, including unsolicited commercial messages or solicitations substantially similar in content. This includes a prohibition against hosting material or electronic mailboxes which facilitate or are used in Spamming.
- **Block Removal:** If Client actions or the actions of their Users have caused Terenine servers or Terenine IP address ranges to be placed on black hole lists and other mail filtering software systems used by companies on the Internet, the Client will be assessed a reasonable fee for administrative charges incurred to remove and protect mail servers and IP ranges.
- **Inappropriate Posting:** Posting or sending messages, articles or other content to a Discussion Group or Forum which are off-topic according to the charter or other Owner published FAQ's or descriptions of the List.
- **Altering Transmission Information:** Falsifying, omitting or misrepresenting transmission information provided to Terenine or engaging in any activities intended to hide a Client's or its User's identity or contact information. This includes forging of any TCP-IP packet header or any part of the header information in an E-mail or a Newsgroup posting.
- **Illegal Activities:** Engaging in any other activity that violates a law or regulation. Prohibited activities include, but are not limited to:
 - Libel, slander, invasion of privacy, harassment, threats, defamation, obscenity, child pornography, export laws and regulations, and infringement or misappropriation of another party's intellectual property.
 - Activities that threatens the integrity and/or security of any network or computer system including, but not limited to, transmission of worms, viruses and other malicious codes and accessing any device or data without proper authorization.
 - Engaging in deceptive online marketing practices or schemes including, without limitation, practices that violate United States Federal Trade Commission Guidelines, e.g., phishing.
 - Attempts to use Terenine services in such a manner so as to avoid incurring required usage charges.
- Any activity that degrades or interferes with other Users' use of a service.
- Activities that breach a third party Non-Disclosure Agreement or obligation. For example, denial of service attacks, web page defacement, port and network scanning and unauthorized system penetrations.
- Unauthorized access to or use of data, systems or networks including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the Owner of the system or network. This prohibition includes attempting to circumvent authentication or security of any host, network or account, e.g., cracking.

- Unauthorized monitoring of data or traffic on any network or system without express authorization of the Owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- High-Risk Activities: The Services are not designed or licensed for use in hazardous environments requiring fail-safe controls, including without limitation, in the operation of nuclear facilities, aircraft navigation/communication systems, air traffic control, life support or weapons systems, and the like.

4. Security

Violations of system or network security, including the prohibited activities listed above, are prohibited and may result in criminal and civil liability.

Users of Terenine's services are responsible for configuring their systems with at least basic security to prevent its use by others in a manner that violates this policy. For example, the Client should properly secure mail servers and FTP servers. Clients are responsible for taking corrective actions to prevent continued abuse.

5. Password Protection

Clients and their Users are responsible for keeping their passwords and account information secure. Clients may not permit anyone unauthorized access to or use of Terenine's services, systems, assets or data. Passwords or User accounts may not be shared with any other party.

Clients and Users are responsible for misuse of the Client or User account, even if the inappropriate activity was committed by a friend, family member, guest or employee.

The Client is required to notify Terenine immediately regarding any unauthorized use of accounts, services or any other breach of security or suspected breach of security.

6. Rights and Remedies

In order to guarantee the Information Systems security of the Client Company, Terenine and all Terenine's Clients and all data exchanged by Users may be audited at any time.

Terenine will investigate any incidents involving violations of this Acceptable Use Policy, as well as disruptions or security breaches and will involve law enforcement if a criminal violation is suspected.

Terenine will cooperate fully with government entities with proper jurisdiction and authorization while investigating unlawful activity on or via our systems or connections. In those instances involving child pornography Terenine complies with all applicable Federal and/or State laws, including providing notice to the National Center for the Missing and Exploited Children or other agencies, as required.

In most cases, Terenine will inform the Client of activities that are in violation of this Acceptable User Policy. However, in cases of immediate threat to Terenine or to its Clients, Terenine reserves the right to disable service or terminate service and/or to

Acceptable Use Policy: POL 0014

remove content in order to investigate suspected violations of this policy or of the Terms of Service, without first giving notice. In addition, Terenine reserves the right to suspend service without notification if it is suspected that the service is the target of an attack or interferes with services provided to other Clients.

The cost of any investigation will be charged to the Client at \$99 USD per hour in addition to charges for attorneys' fees and related expenses, if any. Terenine reserves the right to seek damages for any incidents of unlawful or unauthorized usage of its systems or connections. Terenine does not issue refunds for terminating services due to any of the causes specified above or due to any other violations of this Acceptable Use Policy.

7. Reference Documents

Doc #	Document Name	Region
POL 0007	Security Policy	Terenine