|  |  |  |
| --- | --- | --- |
| Document ID  **ITAD107** | Title  **COMPUTER AND Internet Usage Policy** | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

**Policy:** All employees using the Company Information Technology network shall adhere to strict guidelines concerning appropriate use of network resources.

**Purpose:** To delineate policies and procedures for accessing the Company Information Technology network and/or accessing the Internet through the Company Information Technology network.

**Scope:** This policy applies to all employees with access to Internet and related services through the Company network infrastructure. Internet Related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (email), File Transfer Protocol (FTP), and World Wide Web (WWW) access.

**Responsibilities:**

All Employees are responsible for knowing and adhering to this usage policy.

The Information Technology Security Manager[[1]](#footnote-1) is responsible for enforcement of this policy.

**Definitions:** Internet – The international computer network of networks that connect government, academic and business institutions; the Internet (capitalized) refers specifically to the DARPA Internet and the TCP/IP protocols it uses.

Intranet – A private network contained within an enterprise; a network within one organization, using Web technologies to share information internally.

**Procedure:**

### 1.0 ACCEPTABLE USE - COMPUTERS AND INTERNET

* Access to the Internet is specifically limited to activities in direct support of official Companybusiness.
* In addition to access in support of specific work related duties, the Company Internet connection may be used for educational and research purposes.
* If any user has a question of what constitutes acceptable use he/she should check with their supervisor for additional guidance. Management or supervisory employees shall consult with the Information Services Manager for clarification of these guidelines.

### 2.0 INAPPROPRIATE USE - COMPUTERS AND INTERNET

* Internet access shall not be for any illegal or unlawful purpose. Examples of this are the transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful materials
* Use of Company email or other messaging services shall be used for the conduct of Company business only. These services shall not be used to harass, intimidate or otherwise annoy another person.
* The Internet shall not be accessed for private, recreational, or any non-company-related activity.
* The Company’s intranet or Internet connections shall not be used for commercial or political purposes.
* Employees shall not use Company network for personal gain such as selling access of a Company user login ID. Internet access through the Company network shall not be for or by performing unauthorized work for profit.
* Users shall not attempt to circumvent or subvert security measures on either the Company’s network resources or any other system connected to or accessible through the Internet.
* Company employees shall not use Internet access for interception of network traffic for any purpose other than engaging in authorized network administration.
* Company users shall not make or use illegal copies of copyrighted material, store such material on Companyequipment, or transmit such material over the Company network.

### 3.0 INTERNET AND EMAIL ETIQUETTE

* Company employees shall ensure all communication through Company email or messaging services is conducted in a professional manner. The use of suggestive, vulgar, or obscene language is prohibited.
* Company users shall not reveal private or personal information through email or messaging services without clear and specific written approval from management.
* Users should ensure that email messages are sent to only those users with a specific need to know. The transmission of email to large groups, use of email distribution lists, or sending messages with large file attachments (larger than 0.5 Mb) should be avoided.
* Email privacy cannot be guaranteed. For security reasons, messages transmitted through the Company email system or network infrastructure are the property of the Company and are, therefore, subject to inspection.

### 4.0 COMPUTER AND INTERNET USAGE - SECURITY

* Company users who identify or perceive an actual or suspected security problem shall immediately contact the Information Technology Security Manager, in accordance with procedure ITSD108 – IT INCIDENT HANDLING.
* Network users shall not reveal their account passwords to others or allow any other person, employee or not, to use their accounts. Similarly, users shall not use other employees’ accounts.
* Any and all use of Information Technology assets is subject to monitoring by Information Technology Security.
* Access to Company network resources shall be revoked for any user identified as a security risk or who has a demonstrated history of security problems.

### 5.0 COMPUTER AND INTERNET USAGE - PENALTIES

Any user violating these policies or applicable local, state, or federal laws while using the Company network shall be subject to loss of network privileges and any other disciplinary actions deemed appropriate, possibly including termination and criminal / civil prosecution.

### 6.0 COMPUTER AND INTERNET USAGE - CONCLUSION

All terms and conditions as stated in this document are applicable to all users of the Company network and the Internet. These reflect an agreement of all parties and should be governed and interpreted in accordance with the laws of the country, state, municipality, etc., in which the Company is located.

### 7.0 USER COMPLIANCE WITH USAGE POLICY

The user signifies his or her understanding of the aforementioned policies and agrees to abide by them. The user also signifies understanding that violating these policies is, at the least, unethical and may even be a criminal offense, punishable by revocation of access privileges, disciplinary action (which may include termination), and/or court action that could result in a fine, imprisonment, or both.

Once the user signs form ITAD107-1, they shall deliver the signed original to Human Resources and retain or be given a copy for their personal records.

**Forms:**

* ITAD107-1 COMPANY COMPUTER AND INTERNET USAGE POLICY

**References:**

1. **ISO 27002:2013, INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT**

Clause 8.5.1(c) of ISO 27002 states that “(i)f necessary, special controls should be established to safeguard the confidentiality and integrity of data passing over public networks (i.e., the Internet) and to protect the connected systems...special controls may also be required to maintain the availability of the network services and computers connected.”

ISO 27002 and its companion standards, ISO 27001 and ISO 27005, provide a comprehensive set of controls comprising best practices in the field of information security. The standard treats information as an asset which has value to an organization and, therefore, needs to be suitably protected. Information security protects information from a wide range of threats to ensure business continuity, minimize business damage, and maximize return on investments and opportunities.

NOTE: ISO 27002 was formerly known as “ISO 17799” and before that, BS 7799-2. For more information, see <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>.

**Additional Resources:**

1. None.

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**ITAD107-1 COMPANY COMPUTER AND INTERNET USAGE POLICY**

### Revision \_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### 1.0 ACCEPTABLE USE - COMPUTERS AND INTERNET

* Access to the Internet is specifically limited to activities in direct support of official Companybusiness.
* In addition to access in support of specific work related duties, the Company Internet connection may be used for educational and research purposes.
* If any user has a question of what constitutes acceptable use he/she should check with their supervisor for additional guidance. Management or supervisory employees shall consult with the Information Services Manager for clarification of these guidelines.

### 2.0 INAPPROPRIATE USE - COMPUTERS AND INTERNET

* Internet access shall not be for any illegal or unlawful purpose. Examples of this are the transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful materials
* Use of Company email or other messaging services shall be used for the conduct of Company business only. These services shall not be used to harass, intimidate or otherwise annoy another person.
* The Internet shall not be accessed for private, recreational, or any non-company-related activity.
* The Company’s intranet or Internet connections shall not be used for commercial or political purposes.
* Employees shall not use Company network for personal gain such as selling access of a Company user login ID. Internet access through the Company network shall not be for or by performing unauthorized work for profit.
* Users shall not attempt to circumvent or subvert security measures on either the Company’s network resources or any other system connected to or accessible through the Internet.
* Company employees shall not use Internet access for interception of network traffic for any purpose other than engaging in authorized network administration.
* Company users shall not make or use illegal copies of copyrighted material, store such material on Companyequipment, or transmit such material over the Company network.

### 3.0 INTERNET AND EMAIL ETIQUETTE

* Company employees shall ensure all communication through Company email or messaging services is conducted in a professional manner. The use of suggestive, vulgar, or obscene language is prohibited.
* Company users shall not reveal private or personal information through email or messaging services without clear and specific written approval from management.
* Users should ensure that email messages are sent to only those users with a specific need to know. The transmission of email to large groups, use of email distribution lists, or sending messages with large file attachments (attachments larger than 0.5 Mb) should be avoided.
* Email privacy cannot be guaranteed. For security reasons, messages transmitted through the Company email system or network infrastructure are the property of the Company and are, therefore, subject to inspection.

### 4.0 COMPUTER AND INTERNET USAGE - SECURITY

* Company users who identify or perceive an actual or suspected security problem shall immediately contact the Information Technology Security Manager, in accordance with procedure ITSD108, IT INCIDENT HANDLING.
* Network users shall not reveal their account passwords to others or allow any other person, employee or not, to use their accounts. Similarly, users shall not use other employees’ accounts.
* Any and all use of Information Technology assets is subject to monitoring by Information Technology Security.
* Access to Company network resources shall be revoked for any user identified as a security risk or who has a demonstrated history of security problems.

### 5.0 COMPUTER AND INTERNET USAGE - PENALTIES

### Any user violating these policies or applicable local, state, or federal laws while using the company network shall be subject to loss of network privileges and any other disciplinary actions deemed appropriate, possibly including termination and criminal and/or civil prosecution.

### 6.0 COMPUTER AND INTERNET USAGE - CONCLUSION

All terms and conditions as stated in this document are applicable to all users of the Company network and the Internet. These reflect an agreement of all parties and should be governed and interpreted in accordance with the laws of <State>.

### 7.0 USER COMPLIANCE

I understand and will abide by the Company computer, network, and Internet use policies. I further understand that any violation of this policy is considered unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary action and/or appropriate legal actions may be taken.

User Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_

[This page intentionally left blank]

1. Also “IT Security Manager”, “Information Security Manager”, “InfoSec Manager” [↑](#footnote-ref-1)