# Information Security Policy

## Introduction

Computer information systems and networks are an integral part of business at Imagine!. The company has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

1. Protect this investment.
2. Safeguard the information contained within these systems.
3. Reduce business and legal risk.
4. Protect the good name of the company.

## Violations

Failure to observe these guidelines may result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s). Violations of these policies can lead to revocation of system privileges, e-mail account restriction and/or disciplinary action, up to and including termination.

## Administration

The Director of Information Technology (IT Director) and Information Technology Department personnel are responsible for the administration of this policy. Questions about this policy may be directed to the Director of Information Technology.

## Contents

The topics covered in this document include:

1. Statement of responsibility
2. Internet security and use
3. Electronic mail (e-mail) security and use
4. Information dissemination
5. Computer viruses
6. Access codes and passwords
7. Physical security
8. Copyrights and license agreements

# 1. Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

## Manager responsibilities

Managers and supervisors must:

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

## IT department responsibilities

The IT department must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

# 2. Internet Security and Use

## Purpose

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of Imagine! information and equipment by Internet connections.

## Scope

This policy applies to all employees, contractors, consultants, temporaries, and other users at Imagine!, including those users affiliated with third parties who access Imagine! computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by Imagine!.

## Specific policy

**Introduction**

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes Imagine!'s official policy regarding Internet security. It applies to all users (employees, contractors, temporaries, etc.) who use the Internet with Imagine! computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with Imagine!. All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the IT director.

**Downloaded software**

All software downloaded from non-Imagine! sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

**Information protection**

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, Imagine! confidential, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. The PGP (pretty good privacy) encryption algorithm, or another algorithm approved by the Imagine! IT Director, must be used to protect these parameters as they traverse the Internet. Most web sites will use a secure, encrypted page when the user is expected to submit sensitive information.

Imagine! documentation and all other types of internal information must not be sold or otherwise transferred to any non-Imagine! party for any purposes other than business purposes expressly authorized by management.

**Resource usage**

Imagine! management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not company, time. The use of Imagine!'s internet connection for the streaming of videos and/or music for personal enjoyment is prohibited during business hours, currently Monday-Friday 8:00AM to 4:30PM. Likewise, games, news groups, and other non-business activities must be performed in such a manner so as not to affect productivity.

**Public representations**

Staff may indicate their affiliation with Imagine! in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address. In either case, whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of Imagine!.

Staff must not publicly disclose internal Imagine! information via the Internet that may adversely affect the company's customer relations or public image unless the approval of the department director or executive director has first been obtained.

**Access control**

All users wishing to establish a connection with Imagine! computers via the Internet must authenticate themselves at a firewall before gaining access to the internal network. This authentication process must be done via a dynamic password system approved by the IT Director.

Unless the prior approval of the IT Director has been obtained, staff may not establish Internet or other external network connections that could allow non-Imagine! users to gain access to company systems and information. These connections include the establishment of multi-computer file systems, virtual private network, Internet home pages, FTP servers, and the like.

**Employee responsibilities**

Imagine! is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk.

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or

other form of electronic communication (such as bulletin boards, newsgroups, or chat groups) or displayed on or stored in Imagine!'s computers. Users viewing or receiving this kind of material should immediately report the incident to their supervisors.

# 3. E-mail Security and Use

## Purpose

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.

## Scope

These policies apply to Imagine! employees and contractors and cover e-mail located on Imagine! personal computers and servers if these systems are under the jurisdiction and/or ownership of Imagine! or designated agent(s). These policies apply to stand-alone personal computers and laptops with dial-up modems as well as those attached to networks.

## Specific policy

**Company property**

As a productivity enhancement tool, Imagine! encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Imagine!, and are not the property of users of the electronic communications services.

**Authorized usage**

Imagine! electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as it does not consume more than a trivial amount of resources, interfere with staff productivity or preempt any business activity.

Users are forbidden from using Imagine! electronic communications systems for private business activities. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

**Default privileges**

Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. For example, end users must not be able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of the IT Department has been obtained.

**User separation**

These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user-IDs and associated passwords to isolate the communications of different users. All Imagine! staff and authorized contractors have unique usernames and passwords to access the e-mail system.

**User accountability**

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms.

**No default protection**

Employees are reminded that Imagine! electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. See the IT Director if this requirement is needed.

**Respecting privacy rights**

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. Imagine! is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

The computers and computer accounts given to users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system.

**No guaranteed message privacy**

Imagine! cannot guarantee that electronic communications will be private. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allow authorized IT Department employees to access and review all materials users create, store, send, or receive on the computer or through the Internet or any other computer network. Personal information could and may be deleted.

Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Furthermore, others can access electronic communications in accordance with this policy.

**Regular message monitoring**

It is the policy of Imagine! NOT to regularly monitor the content of electronic communications. However, Imagine! has the right, but not the duty, to monitor any or all aspects of its computer system, including, but not limited to, e-mail sent and received by users. The content of electronic communications and the usage of electronic communications systems may be monitored to support operational, maintenance, auditing, security, and investigative activities. Users understand that Imagine! may use automated software to monitor material created, stored, sent or received on its computer network.

**Statistical data**

Consistent with generally accepted business practice, Imagine! collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, IT staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

**Incidental disclosure**

It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels (department director, executive director, etc.).

**Message forwarding**

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Imagine! sensitive information must not be forwarded to any party outside the company without the prior approval of a department director or executive director.

**Purging electronic messages**
Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. Unless directed to the contrary by your supervisor, inactive e-mail should be discarded after 30 days. Not only will this increase scarce storage space; it will also simplify record management and related activities. If Imagine! is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the executive director or designated representative has communicated that it is legal to do so.

# 4. Information Dissemination

## Purpose
This policy statement provides guidelines for the storage, transfer and security of electronic information resident on personal computers and servers.

## Scope
These policies apply to any electronic data on all personal computers, network and non-network attached, and servers if these systems are under the jurisdiction and/or ownership of Imagine!.

## Specific policy
**Information ownership**
All information travelling over Imagine! computer networks that has not been specifically identified as the property of other parties will be treated as though it is a Imagine! corporate asset. It is the policy of Imagine! to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is the policy of Imagine! to protect information belonging to third parties that has been entrusted to Imagine! in confidence as well as in accordance with applicable contracts and industry standards.

**Location and posting**
Users must not place Imagine! material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless their supervisor or IT Director has first approved the posting of these materials. All publicly writable (Common/Public) directories on Imagine! Internet-connected computers will be reviewed and cleared periodically. Examples include pirated software, out-of date or temporary files and inappropriate written or graphic material (i.e., erotica).

# 5. Computer viruses

## Purpose
The purpose of this policy is to provide for the prevention of infiltration and subsequent spreading of computer viruses or programs designed to make unauthorized changes to programs and data.

## Scope
This policy applies to all employees, contractors, consultants, temporaries, and other users at Imagine!, including those users affiliated with third parties who access Imagine! computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by Imagine! or it’s agents.

## Specific policy

**Background**

It is important to know that viruses can cause substantial damage to computer systems. Computer viruses are much easier to prevent than to cure. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

**Information Systems department responsibilities**

IT personnel shall install and maintain appropriate antivirus software on all computers. IT personnel will respond to all virus attacks, destroy any virus detected, determine spread and document each incident.

**Employee responsibilities**

Employees shall not knowingly introduce a computer virus into company computers. Employees shall not load diskettes or other magnetic or optical media of unknown origin and all incoming media shall be scanned for viruses before they are read. Any e-mail attachments that are suspect should not be opened without first consulting IT personnel. Automated virus scanning on the workstation will detect and clean viruses as the files containing those viruses are opened. In order to assure the virus detection software is current, users must update their virus signature files in accordance with the current procedures. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to the Imagine!'s computers must be scanned. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IT Department.

# 6. Access codes and passwords

## Purpose

The purpose of this policy is to provide for the secure access to all Imagine! shared network resources including data and e-mail.

## Scope

This policy applies to all employees, contractors, consultants, temporaries, and other users at Imagine!, including those users affiliated with third parties who access Imagine! computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by Imagine! or its agents.

## Specific policy

**Background**

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. These access controls can be found, and control access to, workstations, local area networks, wide area networks, remote dial-up connections, individual files, voice mail and e-mail accounts.

**IT responsibilities**

The IT Department shall be responsible for the administration of access controls to all company computer systems. The IT Department will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor. Deletions may be processed by an oral request prior to reception of the written request. The IT Department will maintain a list of administrative access codes and passwords and keep this list in a secure area.

**User Responsibility**
Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be given to others. Users are responsible for all transactions made using their passwords. No user may access the computer system using another user's password or account or disguise their identity while using the computer system. Users should log out when leaving a workstation for an extended period.

**Supervisor's responsibility**
Managers and supervisors should notify the IT Department promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

**Regular password changes**
The IT Department will implement and maintain a system of periodic and automatic password changes on systems that support such processes. These currently include the local area network access and voice mail access. LAN and voice mail passwords need to be changed every six months.

**Passwords do not imply privacy**
Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that users should have an expectation of privacy in the material they create or receive on the computer system. The Imagine! has global passwords that permit it access to all material stored on its computer system-regardless of whether that material is encoded with a particular user's password. The Imagine! has the right to inspect, without prior notice, all material stored on its computer system.

# 7. Physical security

## Purpose
It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

## Scope
This policy applies to all employees, contractors, consultants, temporaries, and other users at Imagine!. The policy also applies to all computer and data communication systems owned by and/or administered by Imagine! or it's agents and the data stored, in electronic, magnetic or optical media, on those systems.

## Specific policy
**Employee responsibilities**
The directives below apply to all employees:

1. Diskettes and other magnetic and optical media should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Diskettes and other magnetic and optical media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). A surge suppressor should protect all other computer equipment.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided. This includes "loaner" systems or laptops that are owned by Imagine! and used at an employee's residence.
5. Since the IT Department is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities unless

specifically instructed by IT Department personnel. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
6. Employees shall not take shared portable equipment such as laptop computers out of the building without the informed consent of the person designated to do so for the department. Informed consent means that the department designee knows what equipment is leaving, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

# 8. Copyrights and license agreements

## Purpose

It is the policy of Imagine! to comply with all laws regarding intellectual property.

## Scope

This directive applies to all software that is owned by Imagine!, licensed to Imagine!, or developed using Imagine! resources by employees or vendors.

## Specific policy

**Legal reference**

Imagine! and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose Imagine! and the responsible employee(s) to civil and/or criminal penalties.

Imagine! strongly supports strict adherence to software vendors' license agreements. When at work, or when Imagine! computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Imagine! work, and are therefore prohibited.

**Information Technology Department responsibilities**

The IT Department will maintain records of software licenses owned by Imagine!. Periodically (at least annually) scan company computers to verify that only authorized software is installed.

**Employee responsibilities**

Without prior authorization from the Information Systems department, users may not do any of the following:

1. Copy software for use on their home computers.
2. Provide copies of software to any independent contractors or clients of the Imagine! or to any third person.
3. Install software on any of the Imagine!'s workstations or servers.
4. Download any software from the Internet or other online service to any of the Imagine!'s workstations or servers.
5. Modify, revise, transform, recast, or adapt any software.
6. Reverse-engineer, disassemble, or decompile any software.

Only software that is licensed to or owned by Imagine! is to be installed on Imagine! computers Employees who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

**Civil penalties**

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

1. Liability for damages suffered by the copyright owner
2. Profits that are attributable to the copying
3. Fines up to $100,000 for each illegal copy

**Criminal penalties**

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the employee(s) responsible to the following criminal penalties:

1. Fines up to $250,000 for each illegal copy
2. Jail terms of up to five years