Immersion Corporation
Cyber Security and IT Policy

Cyber Security and IT Policy

Background

This Immersion Corporation Cyber Security and IT Policy ("**Cyber Security and IT Policy**") is a formal set of rules by which those people who are given access to Immersion Corporation's (and its qualified subsidiaries') technology and information assets (collectively, the "**Immersion Assets**") must abide.

A fundamental component of Immersion's Cyber Security and IT Policy is to protect Immersion Assets from unauthorized access or disclosure. In so doing, Immersion maintains the integrity and availability of its Assets. In order to meet this objective, Immersion must control access to its Assets. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources.

The Director, IT ("**System Administrator**") is responsible for reviewing and approving employee and contractor access to Immersion Assets pursuant to this Policy. The System Administrator will have access to host systems, routers, hubs, and firewalls as required to fulfill the duties of his or her job.

All users of Immersion systems are obligated to protect Immersion's Assets. This information must be protected from unauthorized access, theft and destruction. Immersion's Assets are made up of the following components:

- Business critical information about Immersion's business strategies and operations that others could use to hamper or harm Immersion's business from successfully operating. Examples include customer lists and contact information, contracts, intellectual property, Immersion policy manuals, lab notebooks, strategic plans, and Board meeting minutes.
- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including operating systems, database management systems, and backup and restore software, and communications protocols.
- Application Software used by the various departments within Immersion. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

Threats to Security

- Employees

  One of the biggest threats to information security is a company's employees. Employee actions need not be malicious to put a company at risk; instead,

employees may simply not understand the possible risks associated with their actions. Unauthorized copying of files to portable storage devices, downloading unauthorized software, use of unauthorized P2P file-sharing programs, remote access programs, rogue wireless access points, unauthorized modems, downloading of unauthorized media, and use of personal computing devices for business purposes put the company at risk, including loss of information, security breaches, and legal liability. For example, unauthorized copying of files is a threat as it may lead to loss of confidential information. An employee using his own laptop for business purposes may inadvertently take confidential information home at night or retain this information when he leaves the organization. Downloading unauthorized software or using P2P programs may introduce malware into the organization, leading to theft of information or loss of system availability.

- Amateur Hackers and Vandals.

  These people are the most common type of attackers on the internet. Hacker and vandal attacks are usually crimes of opportunity. Amateur hackers are scanning the internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

- Criminal Hackers and Saboteurs.

  The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

Network Security and Authentication

- Security Infrastructure

  Multi-layered security solutions have been implemented to protect Immersion Assets against malicious activity and cyber-attacks.

  - Network firewalls are configured with anomaly and signature based sensors to protect against advanced threats, including zero day attacks, and provide an advanced intrusion prevention system (IPS).

  - Web security software is installed on all end-user computers to provide real-time malware and zero-day threat protection from web-based attacks.

- Antivirus software is installed on all end-user computers to safeguard against endpoint virus infections.

- All laptop hard drives are encrypted to protect against unauthorized access in case of loss or theft.

- Virtual Private Network (VPN) Access - Telecommuting and Remote Access

  Authorized employees of Immersion are granted permission to access Immersion's network from outside the office, subject to the following:

  - Only authorized persons may remotely access the Immersion network. Remote access is provided to those users who have a legitimate business need to exchange information, copy files or programs, or access computer applications. The only acceptable method of remotely connecting into the internal network is using a secure ID.

  - All VPN (Virtual Private Network) access to the network shall be centrally protected by strong authentication controls. The IT department shall provide procedures to grant access to the VPN.

  - Only machines owned, supported and configured by Immersion IT department must be used for VPN access.

  - Applications that require gateway services must not be installed unless approved and authorized by the IT department (*e.g*. gotomypc, pcanywhere).

  - Employees accessing Immersion's network remotely shall abide by security policies and procedures to protect Immersion's Assets as if the employee were working on the premises.

- Login Security

  - User identification names shall consist of the first initial of first name followed by the last name, *e.g*., jdoe.

  - System and default user names loaded and required by operating systems shall be assigned a password different than what was loaded.

- Passwords

  Passwords are front-line defense against intruders. All users are required to enforce passwords, as follows:

  - Each user account shall have a password. A valid password must meet the following criteria:

- Password must be at least 8 characters long
- Contain characters from 3 of the 4 categories
  - ✓ Uppercase (ABCDEF)
  - ✓ Lowercase (abcdef)
  - ✓ Numbers (12345)
  - ✓ Special Characters (!@#$%^)

o Password will be changed every 120 days.

o The use of last 5 passwords is not permitted.

o The system will prompt the user to change his or her password 14 days prior to its expiration.

Access Control
Immersion has established general principles that help to ensure the appropriate safeguarding of Immersion Assets through logical access controls, such as access codes and passwords.

This Policy covers any Immersion proprietary information or data stored within or processed by an application, system, network, server, personal or handheld computer, or communications device.

General principles governing the appropriate safeguarding of Immersion Information by users are as follows:

- **Access Must Be Requested and Granted Based Upon Approval by Authorized Personnel:** Authorized approval must be requested and granted prior to gaining access to any Immersion Assets at any Immersion location.

- **Restrict Access to the Minimum Level Required:** When requesting or granting access to information, applications, systems, and the network, request or grant the minimum level of access and capabilities required to support relevant work responsibilities and need-to-know.

- **User Accounts Should Not Be Shared:** Sharing of user accounts (user name/password) by multiple users is strictly prohibited without the express approval of the System Administrator.

- **Suspected Disclosure of Passwords:** Users must change (or request the IT department to change) their passwords immediately if they suspect that they have been disclosed to others.

- **Notify the IT Department Promptly Regarding Terminations or Transfers:** The HR department and/or managers and supervisors must notify the IT department promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked or changed. Involuntary terminations must be reported concurrent with the user's termination.

User Responsibilities

Immersion has established a usage policy for its computer systems, networks and information resources. This Policy applies to all users of Immersion's computer systems, networks, and information resources. Each user is responsible for the proper use of any Immersion Assets assigned to him or her or available for his or her use, including password protection and physical control.

User Accounts

User accounts on Immersion computer systems are to be used only for Immersion business and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of Immersion computing systems and facilities may constitute grounds for disciplinary action, including termination of employment, as well as civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Each user must maintain exclusive control over and use of his or her password, and protect it from inadvertent disclosure to others. Passwords should not be recorded where they may easily be obtained. In addition, each user is responsible for all computerized or electronic transactions made with his or her access code and password. Each user must lock or log out when leaving a workstation for an extended period.

Users are prohibited from making unauthorized copies of Immersion Assets and/or distributing it to unauthorized persons.

Users shall not purposely engage in activity with the intent to harass other users, degrade the performance of the system, divert system resources to their own use, use or install spyware, or gain access to Immersion Resources for which they do not have authorization.

Only authorized devices may be connected to Immersion network(s). Authorized devices include computers and workstations owned by Immersion that comply with Immersion's configuration guidelines. Other authorized devices include network infrastructure devices used for network management and monitoring. Users shall not attach unauthorized devices to their computers or workstations, unless they have received specific authorization from the employees' manager and/or an Immersion's IT

department. Users shall not download unauthorized software from the internet onto their computers or workstations.

Users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

Users are required to report any weaknesses in Immersion's computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

All System Administrator passwords will be changed immediately after any employee who has access to such passwords is terminated or otherwise is no longer an Immersion employee.

Employer Property

Computers and other Immersion-owned items are Immersion property and must be maintained according to its rules and regulations. They must be kept clean and are to be used only for work-related purposes. Computer software, including SaaS-based applications, must not be downloaded from the internet and used on an employee's computer without prior authorization from the IT Department. Immersion reserves the right, without notice to the employee and at any time, to inspect all company property to ensure compliance with its rules and regulations. Such inspection may take place outside the employee's presence.

E-mail and the internet

Immersion's computer system, e-mail system, telephone system and voicemail system are to be used for business purposes only and may not be used for private gain or any other commercial purpose. All users shall respect the integrity of technology-based information. Users shall not in any way vandalize equipment either physically or by making the system difficult or unpleasant for others to use. Attempting to crash computers or networks, the creation or intentional use of programs designed to damage computers, the creation or intentional use of programs that inhibit network traffic, the use of chain letters or excessive messages, or devices that restrict legitimate use shall be considered vandalism.

These systems are Immersion's property and are designed to enhance business-related communications. Employee use of the network is considered consent to this policy and to management's right to review e-mail. As such, all messages on Immersion's e-mail system are its property. Immersion reserves the right to access and disclose all messages sent over its electronic mail system and may use information regarding the number, sender, recipient and addresses of messages sent over its electronic mail system for any legal business purpose. While the internet is the embodiment of principles outlined in the First Amendment, some material available on the internet is considered objectionable by many people. This includes, but is not limited to, pornography, "how to" documents encouraging violence or illegal acts and racist tracts

or hate speech. The consequences of accessing and/or disseminating this information will lead to disciplinary actions including possible termination of employment.

Immersion reserves the right to monitor the e-mail network at any time, without prior notice, to ensure that the system is being used for company purposes and to ensure that Immersion policies prohibiting harassment, hostile work environment and other discriminatory conduct are being followed. Employees should disclose information or messages from the e-mail network only to authorized individuals. The implementation and use of the electronic mail system does not in any way modify, amend or alter Immersion's Proprietary Rights Agreement regarding unauthorized use or disclosure of Immersion proprietary of confidential information. Messages containing such information should only be distributed to employees or third parties on a "need to know" basis, and should be appropriately protected (*e.g.*, encrypted) if the recipient is not an Immersion employee.

When an employee sends an e-mail containing Immersion's domain address, that employee is representing the company – not merely himself - in a public medium. All employees must be mindful of the contents of their mail and make certain that it is not harassing or discriminatory, nor is it compromising the legitimate business interests of the company.

Unless otherwise agreed in writing, when an employee leaves Immersion:

- The employee's domain account will be immediately disabled and the employee will no longer have access to Immersion's network or to his/her computer
- No email forwarding to personal email accounts is allowed.
- The employee's supervisor will review the email file and a .PST of approved emails will be made for the employee at his/her request.
- The employee's mailbox on Exchange will be deleted after a final .PST has been created and archived unless internal forwarding has been setup at which time the mailbox will remain active until the forwarding is disabled.
- The employee's computer and user data will be burned to a CD\DVD, archived into the server room, and deleted from the network. An employee may request that IT burn any personal files to a disk for the employee's use. The employee's manager will review and approve this request, and IT will burn the disk.

Internet Usage Policy

Immersion will provide internet access to employees and contractors who are connected to the internal network.

The internet is a business tool for Immersion. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business

partners, obtaining useful business information and relevant technical and business topics.

The internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature, or for any other purpose which is illegal or for personal gain.

This policy covers any service or information accessed through an Immersion-provided internet connection including web pages, personal email accounts, instant messaging, bulletin boards, chat rooms, newsgroups and file/information storage.

- **User Conduct Must Be Honest and Appropriate:** Users must conduct themselves honestly and appropriately on the internet, honoring the acceptable use policies of other networks and respecting the copyrights, software licensing rules, intellectual property rights, privacy and prerogatives of others, just as the individual would in any other business dealings.

- **Internet-based Information Should Be Considered as Suspect:** All information taken from 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 Transmitted or Received Over the internet Is Typically Not Secure:** Information transmitted or received external through the internet should be considered unsecured and vulnerable to third party access. No confidential information should be sent without verifying proper security.

- **Monitoring and Privacy:** The Company has software and systems in place to monitor and record all internet usage. Company security systems are capable of recording each Web site and e-mail message into and out of internal networks. No user should have any expectation of privacy as to his or her internet usage. All messages created, sent or retrieved over the internet are the property of the Company and *may be regarded as public information*. We reserve the right to monitor and record internet usage at anytime if the Company believes, in its sole judgment, that it has a business need to do so.

Authorized Use

Immersion's internet connection is intended primarily for business use. That means that the company expects users to use their internet access primarily for business-related purposes. Specific examples of authorized use include utilizing internet connections and access to carry out day-to-day job duties; communicate with customers, suppliers and other business contacts; research business-relevant topics; and obtain useful business information

Unauthorized Use
Users must not use the internet for purposes that are illegal, unethical, harmful to the company or nonproductive. Specific examples of prohibited use include:

- Participating, during or outside the user's employment. in any internet, online or other electronic bulletin or message board regarding the Company is prohibited, and under no circumstances may any internet, online or other electronic bulletin board or message board posting regarding the Company ever be issued (whether in response to a prior posting regarding the Company or for any other reason whatsoever). Participating, during or outside the user's employment, in any internet, online or other electronic chat room discussion regarding the Company is also prohibited.

- Utilizing peer-to-peer services such as Kazaa, Napster, and bit-torrent programs and sites.

- Downloading of games, e-mail enhancements, graphics or other non-business related applications.

- Downloading or distributing copyrighted material without express authorization from the System Administrator.

- Disabling the security software.

- Excessive use of sports, entertainment and job information and/or sites.

The preceding list of prohibited actions is by way of an example only and is not intended to be exhaustive.

Electronic and Voice Communications Usage Policy
Electronic communications services and underlying technologies (especially internet connections) offer an opportunity for non-authorized individuals to view or access corporate information. Therefore, it is critical that all services and their associated connections be secure, controlled and monitored. The purpose of this policy is to establish general principles along with specific examples of authorized and unauthorized use that ensure that the Company's electronic and voice communications services are utilized in a productive, secure manner.

The Company considers electronic communications services to include e-mail, instant messaging and fax and the underlying technologies to be anything that enables electronic messages to be transmitted, received, processed or stored including internet connections, networks, personal computers, Blackberries, Personal Digital Assistants (PDA's), handheld computers and cellular phones. Voice communications services are considered to be any technology used to transmit, receive, process or store voice messages such as telephones, cellular phones and voice mail.

General principles governing the acceptable use of Company electronic and voice communications services are as follows:

- **Professional Image:** When composing electronic messages, the Company expects users to follow the same standards required in written business communications for the Company. Spelling and grammar in e-mail messages should be checked by the e-mail client before sending the message.

- **Large E-mails Slow System Performance:** E-mail messages containing large attachments, images, etc. can drastically slow system performance. Attachments that exceed 25 MB in size may be removed by the server and not sent.

Unauthorized Use

Users must not use Company-provided electronic and voice communications services for purposes that are illegal, unethical or harmful to the Company or nonproductive. Specific examples of prohibited use include:

- Using Company electronic and voice communications services for private business activities or amusement/entertainment purposes without the express authorization of an authorized member of management of the Company.

- Creating, forwarding or exchanging SPAM (i.e. unsolicited "junk" e-mail sent to large numbers of people to promote products or services), chain letters or e-mails (i.e. messages containing instructions to forward the message to others), solicitations or advertising.

- Sending or forwarding messages that can be perceived as a threat or bullying or as denigrating a person's ethnicity, religion, politics, race, sexual orientation, marital status, age, or disability.

- Making unreasonable use of personal internet service e-mail accounts.

The preceding list of prohibited actions is by way of an example only and is not intended to be exhaustive.

Penalty for Security Violation

Immersion takes the security of its Assets seriously. Any employee or contractor who uses Immersion's Assets must be aware that he or she can be disciplined if he or she violates this Cyber Security and IT Policy. Upon violation of this Policy, the user may be subject to discipline up to and including termination. The specific discipline imposed will be determined on a case-by-case basis, taking into consideration the nature and severity of

the violation of this Cyber Security and IT Policy, prior violations of the Policy committed by the individual, state and federal laws, and all other relevant information.

Immersion also may refer the user to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against it.

Security Incident Handling Procedures

Employees who believe any Immersion Resource has been improperly accessed or used should report the situation to their manager and the IT department immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the issue was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

Acknowledgment

I confirm that I have received a copy of the Immersion Corporation Cyber Security and IT Policy and agree to comply with the terms, conditions and obligations set forth herein.

Employee's Signature: _____

Date: _____