

# U. S. Epperson Underwriting Company Guest Agreement to Comply with Information Security Policies

---

## 1. Overview

Information and information systems are necessary during the performance of most activities at U. S. Epperson (the Company). If there were to be a serious security problem with our information systems, the Company could suffer significant adverse consequences including lost customers, reduced revenues, fines, and/or degraded reputation. As a result, information security must be a critical part of the Company business environment. The Company is committed to protecting its information systems from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of every Information Systems User. It is the responsibility of every User to know these policies and guidelines and to conduct their activities accordingly.

## 2. Purpose

The purpose of this policy is to define baseline control measures which everyone at the Company is expected to be familiar with and consistently follow. These minimum security measures are required to prevent a variety of problems including fraud, industrial espionage, sabotage, unauthorized disclosure of company information, errors and omissions, privacy violations, and system unavailability. This document provides a definitive statement of information security policies to which all users of Company information systems (hereinafter referred to as "Users") are expected to comply.

## 3. Scope

Responsibility for information security on a day-to-day basis is every User's duty. All Company Systems Users are subject to the information security policies and guidelines outlined in this document. This policy applies to all technology equipment and information that is owned or leased by, or entrusted to, the Company.

## 4. Definitions

- 4.1. "Company Information" or "Information" means all information owned by or entrusted to the Company in tangible form.
- 4.2. "Company Information Systems" or "Company Systems" or "Systems" means all computers, servers, printers, scanners, input devices, output devices, network devices, cables, modems, telecommunications lines, telephones, fax machines, telephone systems, security devices, software, applications, computer code, and accompanying documentation that is owned or leased by the Company or entrusted to the Company by a third party.
- 4.3. "User" or "Users" means any person that uses or accesses Company Information and/or Company Systems. A User is typically a Company employee. But a supplier, contractor, customer or partner also may be a Company system User. Adherence to these defined policies applies equally to all users – employees or non-employees.

## 5. Intellectual Property Policy

Information is an important Company asset. Accurate, timely, and properly protected information is absolutely essential to the Company's business.

### **5.1. Legal Ownership of Information**

With the exception of material clearly owned by third parties, the Company has legal ownership of all files, messages, and records stored or transmitted on its Systems.

### **5.2. User Privacy**

All messages and files sent over Company Systems are the property of the Company. To properly maintain and manage this property, management reserves the right to examine all information stored in or transmitted by Company Systems.

The Company does not frequently nor arbitrarily monitor individual Users' activity. However, the Company has the right to monitor User activity, and Users shall consent to be monitored. The Company's failure to monitor activity under certain circumstances in the past does not waive the right of the Company to monitor under similar circumstances in the future.

### **5.3. Recovery of Computer-Related Property Belonging to the Company**

Users must return all hardware, software, working materials, confidential information, and other property belonging to the Company upon request.

### **5.4. Handling of Third Party Confidential and Proprietary Information**

Unless otherwise specified by contract, all confidential or proprietary information that has been entrusted to the Company by a third party must be protected as though it was Company-owned information.

### **5.5. Use of other Organization's Trademarks and Service Marks**

Company communications (web site, brochures, or any other information intended for public consumption) must not use any other organization's trademarks or service marks anywhere unless advanced written permission has been obtained from the Company's Communications Department.

### **5.6. Adherence to Third-Party Software License Agreements**

The Company strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Making unauthorized copies of copyrighted software is prohibited.

### **5.7. When Making Additional Copies of Software is Permissible**

Third-party software in the possession of the Company must not be copied unless such copying is consistent with relevant license agreements and either (a) management has previously approved of such copying, or (b) copies are being made for contingency planning purposes by authorized contingency planning personnel.

### **5.8. If Data security may have been compromised**

In the case your computer or USE data was accessible to non-authorized personal (i.e. intrusion, theft, virus) USE must be notified immediately

## **6. System Access Control Policy**

### **6.1. Access Philosophy**

Access to non-public Company Information Systems is restricted with access controls that discriminate by User.

### **6.2. All Users must be Positively Identified for System Usage**

All users must be positively identified prior to being able to use any Company Information System. This involves identifying yourself to the System using your assigned user-ID and personal password. Initially, new users will have a password assigned to them, and the System will require new users to change their password at first logon.

### **6.3. Signed Forms Required for Issuance of User ID to Non-Employees**

Users who are not Company employees must sign Attachment A to the **U.S. Epperson Underwriting Company Guest Agreement to Comply with Information Security Policies** (F1601) prior to being given a Company Systems user-ID. Users must sign the acknowledgement form indicating they have read and understood these Information Security Policies.

### **6.4. Minimum Password Length**

All user-chosen passwords must have a minimum of 5 alphanumeric characters.

### **6.5. Maximum Password Age**

All user-chosen passwords have an expiration timer. Users are required to change their passwords every 90 days. Users can change their passwords at any time during this 90-day period. Once expired, the System will require the user to change the password immediately before gaining access to Company Systems. Changing passwords regularly maintains the integrity of your user-ID and reduces the risk of unauthorized access.

### **6.6. User-Chosen Passwords must not be Reused**

Users must not construct passwords which are identical or substantially similar to passwords that they had previously employed in the last 6 months.

### **6.7. Writing Passwords Down and Leaving Where Others Could Discover**

Passwords should not be written down and left unprotected. Stored passwords must be sufficiently protected (i.e. locked or password protected)

### **6.8. Limit on Consecutive Unsuccessful Attempts to Enter a Password**

To prevent password guessing by unauthorized parties, the number of consecutive attempts to enter an incorrect password must be limited. After five unsuccessful attempts to enter a password, the involved User-ID will be suspended and must be reset by a System administrator.

### **6.9. Password Sharing Prohibited**

Passwords are our first line of defense against unauthorized access and information disclosure. As such, passwords should be treated like Company-confidential information. Passwords must never be shared or revealed to anyone. To do so exposes the authorized user to responsibility for actions that the other party takes with the password.

### **6.10. Suspected Disclosure Forces Password Change**

A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed to unauthorized parties.

### **6.11. Users Responsible for all Activities Involving Personal User-IDs**

Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with the IDs belonging to other users.

### **6.12. Permission to use Same Password on Different Internal Company Systems**

Users are allowed to use the same password on multiple internal Company Systems. For example, the password used to log-in to the network can be the same as your Company mainframe password; however, the password cannot be the same as a password used to access an email account provided by a third-party such as AT&T or Sprint, even if this account is used only for legitimate Company business purposes.

## **7. Acceptable Use Policy**

Company Systems are provided only for business purposes. Under some circumstances, occasional personal use of Company Systems may be acceptable, provided that no Company policies are violated. Under no circumstances is a worker of the Company authorized to engage in any activity that is illegal under provincial, federal, or international law while utilizing Company Systems.

DISCLAIMER: The Internet is a collection of millions of web sites that contain a variety of information in various forms (text, pictures, audio, video, email, etc.). Some of this information may be considered obscene or offensive. Although willfully searching for, viewing, or storing offensive or obscene information is prohibited, it is virtually impossible to avoid at least some contact with obscene or offensive information. Even innocuous searches for information can return undesired results. Oftentimes, Users may receive unsolicited commercial email (junk mail) that may contain obscene or offensive material. Use the internet at your own risk. The Company is not responsible for content viewed by its Users on the Internet using Company Systems.

### **7.1. Restricted Behavior for Outbound Internet Communications**

All outbound Internet communications (email, chat room remarks, discussion group postings, web form entries, etc.) must reflect well on the Company's reputation and public image. Inflammatory, defamatory, harassing, or disruptive communications are prohibited. Likewise, spamming (sending unsolicited "junk mail") is prohibited. Additionally, forwarding jokes or chain mail is also prohibited.

### **7.2. Gaining Unauthorized Access via Company Information Systems**

Users are prohibited from gaining unauthorized access to any other information system or in any way damaging, altering, or disrupting the operations of other systems, both internal and external. Likewise, workers are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

### **7.3. Misrepresentation of Identity on Electronic Communication Systems**

Misrepresenting, obscuring, suppressing, or replacing your identity on an electronic communications system is forbidden. The username, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

**7.4. Restriction against Using Computer Hardware or Software not owned by the Company**

The use of non-USE owned hardware or software, will be at the user's risk, and Company will not be responsible for data loss or any damage to non-USE-owned equipment, hardware, software, or data.

Within our corporate offices, suppliers, contractors, or customers who desire to connect to our corporate network must have their computer examined by a member of the Help Desk or Network Services prior to attaching directly to our network. Failure to comply with this requirement breaches our antivirus and information security protection measures and consequently puts all our systems and information at risk.

**7.5. Existence of User Access Capabilities does not Imply Usage Permission**

Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file. Unless general user access is clearly provided, the ability to read, modify, delete, or copy a file belonging to another user does not imply permission to actually perform these activities.

**7.6. Prohibition against Testing Information System Controls**

Users must not test or attempt to compromise internal controls unless this activity is part of the User's job description.

**7.7. Prohibition against Exploiting Systems Security Vulnerabilities**

Users must not exploit vulnerabilities or deficiencies in information systems security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other Users, or to gain access to other Systems for which proper authorization has not been granted. All such vulnerabilities and deficiencies should be promptly reported to management.

**7.8. Tools Used to Compromise Systems Security Prohibited**

Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those which eavesdrop on data transmissions, defeat software piracy protection, discover secret passwords, identify services or vulnerabilities, or decrypt encrypted files.

**7.9. User Installation of Software on USE owned Computers is Prohibited**

Users must not install software on computers, network servers, or other machines without first receiving advance authorization to do so from the IT Department.

**7.10. Users Prohibited from Upgrading Software on USE owned Computers**

Unless previously authorized by IT management, users are prohibited from installing new or upgraded programs on their computers.

### **7.11. User Changes to Operating Systems is Prohibited**

Extensions, modifications, or replacements to production operating system software must only be made by the IT Department.

### **7.12. Users Prohibited from Installing, Connecting, Disconnecting, Removing, or Changing Computer Hardware on USE owned computers**

Unless authorized by the IT Department and while in communication with the IT Department or the Help Desk, users cannot install, connect, disconnect, remove, or change any hardware component inside or attached to any Company-owned computer. This list of hardware includes but is not limited to printers, scanners, digital cameras, PDAs, PocketPCs, monitors, mice, keyboards, speakers, microphones, sound cards, video cards, network cards, modems, hard disk drives, removable disk drives, etc.

## **8. Anti-Virus Policy**

Computer viruses, worms, trojans, malicious code, spyware, and ad-ware (hereinafter collectively known as "viruses") are unauthorized programs which replicate themselves and spread onto various data storage media and/or across a network. The symptoms of virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, and total failure of a computer system. They can disrupt computer and network services, collect and transmit Company Information to unauthorized third parties, and/or allow unauthorized access to Company Systems. Globally, about six new viruses are discovered daily.

### **8.1. Never Open Email File Attachments from Unknown Sources**

Users must never open files attached to an email message from unknown, suspicious, or untrustworthy sources. They must also delete these emails immediately then delete again by removing from your "trash" or "deleted items" folder.

### **8.2. Delete Junk Emails without Forwarding**

Users must always delete spam, chain, jokes, and other junk emails without forwarding or replying. If this type of unwanted email persists, contact the Help Desk.

### **8.3. Never Respond to Unsolicited Junk Emails**

Users must never respond to unsolicited junk emails. This includes responding to offers to have your email address removed from the sender's list. Responding to these offers generally increases the amount of unsolicited junk emails that the User receives and is oftentimes an avenue for viruses.

### **8.4. Prohibition against Downloading Software from Third Party Systems**

Users must not download software from electronic bulletin board systems, the Internet, newsgroups, or any other system outside of the Company. This prohibition is necessary because such software may contain viruses which may damage Company Systems.

#### ***8.5. Always Scan Floppy Disks for Viruses before Using***

Although floppy diskettes are not in widespread use anymore, there are some instances where there may be a legitimate business need to use information on a floppy diskette. Always scan floppy diskettes for viruses before using.

#### ***8.6. Users must not Attempt to Eradicate Computer Viruses on USE owned computers***

Because viruses have become very complex, Users must not attempt to eradicate them without expert assistance from the IT Department or the Help Desk. If Users suspect infection by a virus, they must immediately call the Help Desk. This communication will help minimize damage to data files and software, as well as ensure that information needed to detect a re-infection has been recorded.

#### ***8.7. Approved Virus Checking Programs Required on all Computers and Laptops Connecting to Company Systems***

Company-owned computers must have standard virus-scanning software pre-loaded and running at all times. All personally-owned computers connecting to Company Systems must have Company-approved virus-scanning software loaded and running. All virus-scanning software must have the latest virus database downloaded and installed. The virus database is a list of viruses that the computer is protected against. Since many viruses are discovered daily, virus databases change and must be downloaded regularly.

#### ***8.8. All User Involvement with Computer Viruses Prohibited***

Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any Company computer, network, or information. Such software is known as a virus, worm, trojan, malicious code, spyware, adware, malware, and similar names.

# Attachment A

A signed paper copy of this attachment must be submitted by a U.S.E. employee with all requests for (1) authorization of a new user-ID for non-employees or (2) periodic reauthorization of an existing user-ID for non-employees.

---

## ACKNOWLEDGEMENT OF RESPONSIBILITIES BY NON-EMPLOYEE

I am not an employee of U. S. Epperson Underwriting Company (Company) and I have read and understand the U. S. Epperson Company Guest Agreement to Comply with Information Security Policies. I understand how these policies impact the Company. I agree to abide by these security policies. I understand that non-compliance will be cause for disciplinary action up to and including System privilege revocation, dismissal from Company premises, termination of any business relationship, as well as criminal or civil penalties.

I also agree to promptly report all violations or suspected violations of security policies to the Information Technology Help Desk.

User Printed Name: \_\_\_\_\_

User Department: \_\_\_\_\_

User Company: \_\_\_\_\_

User Signature & Date: \_\_\_\_\_

## ACKNOWLEDGEMENT OF RESPONSIBILITIES BY SPONSOR/EMPLOYEE

I certify that I am an employee of the Company, the individual named above has a legitimate business requirement to gain access to Company Information Systems, and I am authorized to sponsor their access.

U. S. Epperson Employee-Sponsor - Printed Name: \_\_\_\_\_

U. S. Epperson Employee-Sponsor - Department: \_\_\_\_\_

U. S. Epperson Employee-Sponsor – Signature & Date: \_\_\_\_\_