EMPLOYEE & CONTRACTOR INFORMATION SECURITY

JDP Information Security Acceptable Use Policy

Overview

J.D. Palatine Information Security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to J.D. Palatine's established culture of openness, trust and integrity. J.D. Palatine Information Security is committed to protecting J.D. Palatine's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of J.D. Palatine. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review J.D. Palatine Employment Policies Handbook for further details.

Effective security is a team effort involving the participation and support of every J.D. Palatine employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at J.D. Palatine. These rules are in place to protect the employee and J.D. Palatine. Inappropriate use exposes J.D. Palatine to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at J.D. Palatine, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by J.D. Palatine.

Policy

General Use and Ownership

While J.D. Palatine's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of J.D. Palatine. Because of the need to protect J.D. Palatine's network, management cannot guarantee the confidentiality of information stored on any network device belonging to J.D. Palatine.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

J.D. Palatine Information Security recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see J.D. Palatine Information Security's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to J.D. Palatine Information Security's Awareness Initiative.

For security and network maintenance purposes, authorized individuals within J.D. Palatine may monitor equipment, systems and network traffic at any time, per J.D. Palatine Information Security's Audit Policy.

J.D. Palatine reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

It is critical to protect J.D. Palatine's property and information assets. Employees are expected to be aware of and protect the sensitive nature of consumer information, business intellectual property, strategies, etc. In addition, employees are expected to exercise caution in making any statements about products or services.

Confidentiality and Information Protection

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

In keeping with J.D. Palatine clear desk and clear screen policies, all PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended. Do not leave sensitive information displayed on unattended devices.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Use encryption of information in compliance with J.D. Palatine Information Security's Acceptable Encryption Use policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with system administrator instructions and configurations.

Postings by employees from a J.D. Palatine email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of J.D. Palatine, unless posting is in the course of business duties.

All hosts used by the employee that are connected to the J.D. Palatine Internet/Intranet/Extranet, whether owned by the employee or J.D. Palatine, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Any hard copies or other media containing sensitive information that is to be mailed or delivered shall be labeled confidential and then tracked using a secure courier.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Data on paper:

- Employees shall adhere to the following clear desk policy.
- Employees shall label all documents that should be company-confidential using a standard format in page headers or by stamping each page clearly with a warning.
- Company-confidential documents must not be exposed to casual inspection.
- Confidential papers shall be placed in locked cabinets or drawers when their user leaves the work area.
- Employees must exercise care in protecting confidential documents when carrying them out of the facility or using them at home or elsewhere.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Data on disk and tape:

- Diskettes, removable disks, flash drives and tapes containing sensitive information are always to be clearly labeled to indicate their contents.
- All diskettes, removable disks, flash drives and tapes are to be tracked in a media inventory managed by system administrators
- When confidential data are stored on any magnetic or optical medium, the data are to be encrypted using approved software.
- In particular, backup media must store sensitive information in encrypted format, or the organization must provide a safe or similar secure location to store backup media.

Data in RAM and swap files:

- When a computer requires service by non-corporate technicians, it shall be shut down before access.
- If a computer system contains highly sensitive materials, it may be necessary to use a secure wipe or to replace the disk drive(s) containing such data rather than allow outside technicians to have access to the unencrypted data in the operating system swap files.

Data in transit:

- Confidential data being sent outside the organization shall be encrypted in transit.
- Any hard copies or other media that are to be mailed or delivered are to be labeled confidential and then tracked using a secure courier.

Data Deconstruction:

- Confidential information on paper shall be shredded before disposal.
- When erasing confidential files on disks, use wipe utilities to ensure that all data residues are overwritten.
- When disposing of obsolete computer equipment, ensure that the hard disks are completely wiped of confidential data and proprietary software.
- If a disk drive containing confidential data has failed and cannot be overwritten, destroy it physically (e.g., by smashing or incinerating) to prevent uncontrolled data recovery.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Hardware and Software

- Removal or relocation of computing assets requires written approval from the technical support staff.
- Users may install only authorized hardware on their workstations.
- Modems are not authorized and are not to be installed on any computing assets.
- It is a violation of security procedures to disable or modify hardware such as RAM, processors, coprocessors, I/O boards or peripheral equipment without the authorization of technical support staff.
- Users may not interchange components from one workstation to another without authorization and logging of the changes by technical support.
- Users may install only authorized software on their workstations.
- Users must install firewall software on personal laptops authorized for use on the network. System administrators are required to ensure that every laptop or personal system has appropriate firewall and antivirus software installed.
- It is a violation of security procedures to disable or modify security software such as access controls or anti-virus software without the authorization of technical support staff.
- User programs such as spreadsheets that are used for business decisions are production software and must be treated like any other production software regardless of origin, in particular, users must submit to technical support:
- Documentation (usually in the form of explanatory comments)
- Quality assurance test suites with known answers to check calculations and branchpoints
- Backup plans showing frequency and location of backups.
- Limited, occasional, or incidental use of company resources for personal, nonbusiness purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Mobile Computing Devices

- Tablets, and other mobile computing and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain.
- The most effective way to secure confidential data is not to store it on mobile devices. As a matter of policy and best practice data should always be secured where it resides.
- Business requirements may, on occasion, justify storing confidential data on mobile computing devices. In these cases, users are required to assure that steps have been taken to keep the data secure.
- Any mobile computing device accessing or storing restricted/confidential or internal information is subject to all security policies and in addition, will adhere to the following, if the capability exists for the device:
- Receive and install security and other operating system updates from the operating system vendor.
- Use a device and/or screen saver password. Portable computing devices must, at a minimum, be pass word protected.
- Unattended devices must be physically secured.

Anti-virus

- All desktop and laptop PCs must have approved anti-virus software installed, configured, and operational according to the recommended desktop anti-virus software configuration (contact technical support staff for help with configuration):
- Enable full-time, background, real time, auto-protect or similar mode
- Enable start-up scanning of memory, master / boot records, system files
- Enable logs to log all desktop virus-related activity
- Enable anti-virus software heuristic controls (in full-time background mode where available)
- Update anti-virus software virus signatures at least monthly, and within two business days after receiving an alert.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Recommended Microsoft Word configuration:

Configure all instances of MS Word to save files as Rich Text Format (*.rtf). Where needed to reduce the file size of complex documents, or for files that require macro use or other very advanced, embedded features use, *.doc is acceptable.

Locking the Workstation and Screen Saver Usage

- Whenever leaving the workstation, the employee should use CTRL-ALT-DEL to lock the workstation to prevent unauthorized access.
- All desktop and laptop PCs should have a screen saver installed and operational.
- Recommended screen saver configuration:
- Enable screen saver, with password protection. Recomended inactivity delay is no more than 15 minutes.
- Follow a clear screen policy – do not leave the workstation unattended with sensitive information displayed on the screen.

Passwords

- Passwords must not be words found in a dictionary.
- Passwords should have no personal significance for their user (e.g., names of spouses, friends, favorite sports, pets, hobbies and so on are too easy to guess for anyone who does a bit of background checking).
- Passwords should consist of at least six alphanumeric characters, including at least one non-alphabetic symbol (e.g., urto5jelex is a better password than urtojelix).
- Passwords should not merely increment a numerical value from change to change (e.g., urto5jelex followed the next time by urto6jelex is poor choice of passwords).
- Passwords should also avoid:
- 2 or 4-digit year
- 3-character abbreviations for any month
- 3 or more characters in alphabetic order

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

- any string of 3 or more identical characters
- any string or 3 or more characters repeated or reversed
- the user ID itself or its reverse
- When passwords are being keyed, users must be sure that no one is shouldersurfing (observing their keystrokes).
- Anyone near a person entering a password must turn away so as not to observe the keys being used; this element of corporate culture is best modeled by upper management.
- Do not share your password with anyone for any reason. Passwords must be changed immediately when there is any suspicion that they have been compromised.
- Requests from individuals to reset their password should first be authenticated through positive identification of the individual. This may include checking photo ID, verifying personal information, or initiating contact through contact information on file.

Termination Procedures

- An employee who resigns with notice and who is on good terms with the organization may be permitted to complete projects; however, the organization must evaluate and tighten security requirements such as access to data not directly related to the current projects.
- All departing employees will be interviewed by at least two managers, including a representative of the human resources department. The exit interview will include:
- A resigning employee will be asked to explain as much as possible about the reasons for the resignation.
- An employee whose employment is terminated by the employer will be informed of the reasons for termination, given a check for the required period of notice plus any severance pay, and then escorted by facilities security personnel for removal of personal belongings and return of company property.
    - The departing employee shall return corporate property such as
    - Company badges
    - IDs
    - Business cards
    - Credit cards
    - Keys
    - Computers

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

- As the employee is packing and returning property, security management shall:
- Strike the person's name from all security-post lists of authorized access;
- Explicitly inform guards that the ex-employee may not be allowed into the building, whether unaccompanied or accompanied by an employee, without special authorization by named authorities;
- Change the combinations, reprogramming access card systems, and replacing physical keys if necessary for all secure areas to which the individual used to have authorized access;
- Remove or change all personal access codes known to have been used by the exemployee on all secured computer systems (microcomputers, networks, mainframes);
- Inform all outside agencies (e.g., Tape storage facilities, publications with company advertising) that the ex-employee is no longer authorized to access any of the employer's information or to initiate security or disaster recovery procedures;
- Request cooperation from outside agencies in informing the employer if exemployees attempt to exercise unauthorized functions on behalf of their former employer.
- No departing employee shall receive a farewell celebration on corporate premises or at company expense; such celebrations must be organized privately by other employees and held off-site. This restriction ensures that unpopular employees or those leaving under a cloud are not stigmatized — and also reduces the likelihood of lawsuits for defamation.
- In response to requests for a reference on behalf of a former employee, J.D. Palatine shall provide only the factual information on the person's job title(s), functions, and period of service. Additional information may be provided only upon consultation with legal counsel.

Internet Browsing

- Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass the company
- No employee shall use corporate resources to download offensive or illegal materials into the workplace or onto corporate computers or peripherals. Such materials include but are not limited to:
- Pornography of any kind (remembering in particular that producing, downloading, uploading, and/or storing child pornography is a felony)

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

- Hate literature or hateful images
- Illegal copies of software (remembering that it is forbidden to install software of any kind on corporate systems without approval of technical support).
- Company Internet users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening, or racially or sexually harassing.
- Users of the WWW are reminded that Web browsers leave "footprints" providing a trail of all site visits.
- All software used to access the WWW must be approved by the Network Manager and must incorporate all vendor provided security patches.
- Any files downloaded over the WWW shall be scanned for viruses, using approved virus detection software.
- Only company approved versions of browser software may be used or downloaded. Non-approved versions may contain viruses or other bugs.
- When using a form, ensure that the SSL or Secure Sockets layer or other such mechanism is configured to encrypt the message as it is sent from the user's browser to the Web server.
- No sites known to contain offensive material may be visited.
- Any user suspected of misuse might have all transactions and material logged for further action.

Email Usage

- E-mail sent or received using corporate resources is subject to audit at any time. There will be no expectation of privacy by anyone with regards to corporate e-mail.
- All corporate e-mail must be composed with the awareness that it may be exposed to public scrutiny if it is demanded in a legal discovery process.
- Any outbound e-mail sent using a corporate e-mail account is to be considered as equivalent to a message sent on corporate letterhead:
- The content and tone of any such message must reflect the official responsibilities of the author.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Internet Collaboration

- Employees using corporate resources to access the Internet shall comport themselves as representatives of the organization. That is, all messages posted by employees in public or private discussion groups (e.g., USENET groups) shall be:
- Composed in a professional, truthful, non-confrontational style
- Signed with the organizational affiliation and title
- Adding disclaimers about one's opinion not reflecting that of the organization in no way excuses unprofessional behavior.
- Corporate participants in Internet discussion groups on technical issues must explicitly reveal bias related to corporate interests when commenting on any issues, whether positively or negatively.
- When expressing opinions about any products from publicly traded companies, U.S. employees and employees of U.S. corporations are to conform to the requirements of the Securities and Exchange Commission.
- When expressing opinions about any products whatsoever, employees are to avoid libelous comments.

Blogging /Social Networking

- Blogging and/or social networking by employees, whether using J.D. Palatine's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of J.D. Palatine's systems to engage in blogging and/or social networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate J.D. Palatine's policy, is not detrimental to J.D. Palatine's best interests, and does not interfere with an employee's regular work duties. Blogging and/or social networking from J.D. Palatine's systems is also subject to monitoring.
- J.D. Palatine's Confidential Information policy also applies to blogging and/or social networking. As such, Employees are prohibited from revealing any J.D. Palatine confidential or proprietary information, trade secrets or any other material covered by TazWork's Confidential Information policy when engaged in blogging and/or social networking.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

- Employees shall not engage in any blogging and/or social networking that may harm or tarnish the image, reputation and/or goodwill of J.D. Palatine and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging and/or social networking or otherwise engaging in any conduct prohibited by J.D. Palatine's Non-Discrimination and Anti-Harassment policy.
- Employees may also not attribute personal statements, opinions or beliefs to J.D. Palatine when engaged in blogging and/or social networking. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of J.D. Palatine. Employees assume any and all risk associated with blogging and/or social networking.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, J.D. Palatine's trademarks, logos and any other J.D. Palatine intellectual property may also not be used in connection with any personal blogging and/or social networking activity.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of J.D. Palatine authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing J.D. Palatine-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by J.D. Palatine.

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which J.D. Palatine or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a J.D. Palatine computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any J.D. Palatine account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to J.D. Palatine Information Security is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, J.D. Palatine employees to parties outside J.D. Palatine.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Untrue, inaccurate, misleading, obscene, racist, sexist, ad hominem or other unprofessional remarks may make the organization liable for legal action and will be considered a serious breach of professional ethics.
- No employee will use e-mail to knowingly transmit or retrieve any communication that is discriminatory or harassing; derogatory to any individual or group; obscene, sexually explicit or pornographic; defamatory or threatening; in violation of any license governing the use of software; or engaged in for any purpose that is illegal or contrary to J.D. Palatine policy or business interests.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within J.D. Palatine's networks of other Internet/Intranet/
- Extranet service providers on behalf of, or to advertise, any service hosted by J.D. Palatine or connected via J.D. Palatine's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

EMPLOYEE & CONTRACTOR INFORMATION SECURITY

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, criminal prosecution or civil action.

Definitions

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Social Networking	Posting commentary, photos, media, links, etc. to a social networking service, such as Twitter, Facebook, MySpace, LinkedIn, etc.
Spam	Unauthorized and/or unsolicited electronic mass mailings.