



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

USPTO RULES OF THE ROAD OCIO-6016-10

Effective Date: March 2, 2010

Purpose of Revision: Revised rule for saving Federal records; clarification of employee use of the Internet

Review Date:

TABLE OF CONTENTS

Section

- I. Purpose
- II. Authority
- III. Scope
- IV. Policy
- V. Responsibilities
- VI. Effect on Other Policies
- VII. References

I. PURPOSE

PTOnet, USPTO Automated Information Systems (AISs), and other computing resources are shared among USPTO employees. PTOnet provides access to USPTO business systems that operate on the USPTO information technology infrastructure and provides access to remote locations through secure gateways. PTOnet also provides access to the Internet and external news groups.

The PTOnet and USPTO AIS "Rules of the Road" are intended to help you use the USPTO's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to all employees.

Complying with these rules will help maximize access to these facilities and help assure that your use of them is responsible, legal, and respectful of privacy. You must follow the "Rules of the Road" when using USPTO automation resources.

The Rules of the Road are grouped into three categories, as follows:

1. Complying with the intended use of PTOnet and USPTO AISs.
2. Assuring ethical use of PTOnet and USPTO AISs.
3. Assuring proper use of PTOnet and USPTO AISs.

USPTO RULES OF THE ROAD

The following is a more detailed discussion of the individual rules associated with each category. The Rules of the Road are also discussed in appropriate sections of the *USPTO Internet and Intranet Services Guide* and the *USPTO E-Mail User's Guide*. Each USPTO Business Unit may supplement the Rules of the Road for better administration of information within its own organization.

II. AUTHORITY

This policy is issued pursuant to:

- The Federal Information Management Security Act of 2002 (FISMA)
- USPTO IT Security Policy Management Policy

III. SCOPE

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO computer systems, and to employees of contractor systems owned and operated on behalf of the USPTO.

It is important that USPTO employees and contractors understand the purpose of PTOnet and USPTO AIS so that usage of USPTO AIS is in compliance with that purpose.

IV. POLICY

Complying with the Intended Use of PTOnet and USPTO AISS

It is important that you understand the purpose of PTOnet and USPTO AISs so that your use of them is in compliance with that purpose.

Rule #1: Do not conduct unauthorized business on the PTOnet or USPTO Automated Systems.

The purpose of the USPTO is to administer the laws relating to patents and trademarks in order to promote industrial and technological progress in the United States and strengthen the national economy. As a USPTO employee, you have an obligation to conduct your activities in keeping with the USPTO mission, goals, and objectives. All use of PTOnet and USPTO automated systems, including accessing the Internet, must be consistent with this purpose. The following are appropriate uses of the PTOnet and USPTO automated systems:

- Exchange of information that supports the USPTO mission, goals, and objectives.
- Job-related professional development for USPTO management and staff.
- Communications and exchange of information intended to maintain job currency or gain additional knowledge that is directly or indirectly related to job functions.

USPTO RULES OF THE ROAD

- Communications and exchange of information generally supportive of otherwise acceptable uses.

Internet services and e-mail provided by the USPTO during official working hours so long as they are used for authorized purposes only. However, limited personal use of the Internet, including sending infrequent personal e-mail messages, is permissible provided such use is consistent with the Rules of the Road and does not interfere with conducting USPTO business. The privilege to use government equipment for limited personal purposes may be revoked or restricted at any time by the USPTO. USPTO employees should consult with their respective supervisors in case of any doubt about the appropriate use of any government equipment.

The USPTO flexible work schedules, including the Increased Flextime Policy (IFP), and mid-day flex, should minimize the necessity for personal use of any and all government equipment during normal working hours. However, employees are reminded of their obligation to truthfully certify their time and attendance records and to report as duty time only that time spent performing official duties.

Please refer to the USPTO policy AAO 202-735 regarding *Limited Personal Use of Government Equipment* for further details. Other USPTO directive can be found on the USPTO Intranet at <http://ptoweb/ptointranet/directives/index.html>.

All unauthorized use of PTONet and USPTO AISs is prohibited. The following activities, while not an exhaustive list, are specific examples of unacceptable uses of the PTONet and USPTO automated systems:

- Use for commercial purposes, for financial gain, or in support of private business activities.
- Use for posting to or subscribing to external news groups, bulletin boards, or other public forums for personal reasons.
- Initiating actions that interfere with the supervisory or accounting functions of the AIS including attempting to obtain "system" privileges.
- Creating, storing, or sending electronic chain letters.
- Using the Internet or Intranet as a staging ground or platform to gain unauthorized access to other systems.
- Publishing personal opinions using a USPTO Internet user-ID to external (non-PTO) entities without being expressly authorized by individual job description or through clearance from the USPTO (inclusion of a disclaimer that such statements are not those of the USPTO is not sufficient to obviate or negate this restriction).
- Any communications with the media without prior approval of the Office of Public Affairs.
- Engaging in any activity that would discredit the USPTO, including the creation, downloading, viewing, storage, copying, or transmission of sexually explicit and/or

USPTO RULES OF THE ROAD

sexually oriented materials or materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

- In the normal course of AIS operations and maintenance activities, usage of the AIS may be monitored in order to ensure the continued operational effectiveness and integrity of the PTOnet, USPTO AISs, and other computing resources. You are reminded that such monitoring does occur. Of course, unauthorized or improper use of the AIS will be investigated and, when appropriate, official sanctions will be imposed as a result of such use. Likewise, if criminal activity is discovered AIS information will be provided to the appropriate law enforcement officials.

Rule #2: Save Federal Records

The Federal Records Act defines records as *“all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.”* (44 U.S.C. 3301).

Any electronic message (e.g., information transmitted through electronic mail, the Internet, or wireless hand held device) should be treated as if it were a paper document when it comes to determining whether it is a Federal record.

Federal records must be maintained according to an approved disposition schedule. The Comprehensive Records Schedule for the USPTO can be found on the USPTO Intranet.

Use the following guidelines to determine if an electronic message should be considered a Federal record:

- If you take official action related to a message, it is a federal record.
- If the message is needed for adequate and complete documentation of an action you have taken or has been taken in the course of your business, it is a federal record.

You must maintain the body, subject, date transmitted and names of the sender(s) and receiver(s). You also must maintain attachments to an electronic message if that message is a federal record. Federal records must be managed in a proper record keeping system.

Except where an electronic record keeping system exists, electronic messages that are records, including electronic mail records, should be printed to paper and retained in a paper filing system. Where an electronic record keeping system exists, the electronic message or electronic mail record should be retained in that system.

USPTO RULES OF THE ROAD

If you have any questions about the determination or disposition of an electronic message, or need assistance in managing electronic records, please contact your Business Unit's records coordinator or the USPTO Records Officer.

Assuring Ethical Use of PTOnet and USPTO AISS

Along with the many opportunities that PTOnet and USPTO AISs provide for USPTO employees to share information, comes the responsibility to use the AISs in accordance with USPTO standards of conduct. These standards are outlined in the USPTO Employee Handbook. Appropriate use of PTOnet and USPTO AISs includes maintaining the security of the AISs, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

Rule #3: Do not let anyone know your password

While you should feel free to let others know your user name (this is the name by which you are known to the whole PTOnet, USPTO AISs and Internet community), you should never let anyone know your account passwords. This even includes trusted friends.

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the AIS will be traced back to your user name — if your user name or account is used in an abusive or otherwise inappropriate manner, the USPTO will hold you responsible.

When creating or changing your password, always use a password that you can easily remember but is unique enough that it cannot be easily guessed by your co-workers. Never use the names of spouses, children, pets or birthdates, as these can easily be compromised.

Rule #4: Do not violate the privacy of other users

The Electronic Communications Privacy Act (18 USC 2510 et seq., as amended) and other Federal laws protect the privacy of users of wire and electronic communications. The facilities of the PTOnet and USPTO AISs are in place to facilitate the sharing of information among USPTO employees, our international partners, and our customers. As a user of the PTOnet and USPTO AISs, make sure that your actions do not violate the privacy of other users, even if unintentionally.

Some specific areas to watch for include the following:

- Do not try to access the files of directories of another user without clear authorization from that user.
- Do not try to intercept or otherwise monitor any network communications not explicitly intended for you.
- Do not use names or other personal identifiers in communications that might be of a sensitive or confidential nature.

USPTO RULES OF THE ROAD

- Do not intentionally seek information about, browse, obtain copies of, or modify files, mail, or passwords belonging to others, whether they are at the USPTO or elsewhere, unless specifically authorized to do so by those individuals.
- Do not attempt to decrypt or translate encrypted material belonging to another person or organization.
- Do not attempt to alter the “From” line of your Internet user-ID or other attributes of origin in electronic mail, messages, or news group postings.
- Do not edit or change the content of an e-mail message when sending a reply to the message’s originator or forwarding the message to another person without indicating where and how the message was edited.
- Do not create any shared programs that secretly collect information about USPTO users.

Rule #5: Do not transmit classified or sensitive data

Every attempt has been made to ensure that appropriate security mechanisms are in place for protecting information from unintended access, from within the AIS or from the outside. However, these mechanisms, by themselves, are not sufficient. PTONet and USPTO AIS users should ensure that they take appropriate action to safeguard classified or sensitive data. USPTO AIS users are instructed to implement the following requirements:

- Do not transmit classified data, data subject to a secrecy order, or data under seal through the Internet or e-mail, unless it has been properly protected through encryption software.
- Do not store or transmit sensitive data without proper protection as defined in applicable Federal laws and regulations. Sensitive data should not be posted in discussion groups or bulletin boards. Data should be considered sensitive if it might be exempt from Freedom of Information Act (FOIA) disclosure or protected under the Privacy Act. Sensitive data includes records about individuals in which there is a reasonable expectation of privacy, trade secrets or confidential business information, and confidential information related to Patent and Trademark applications.
- Do not transmit data that is part of the USPTO decision-making process over the Internet or in public news groups.
- Do not automatically forward electronic mail, via rule, macro or script. Automatic forwarding potentially creates a serious operational threat and an unjustified risk to confidentiality obligations. Sensitive USPTO information may inadvertently be transmitted and stored in a public medium without protection. Senders using automatic forwarding have no knowledge or control of the content that is being forwarded and have no way to filter sensitive information from being forwarded. Therefore, auto forwarding of e-mail outside the USPTO network is prohibited. Auto-replies or out-of-office settings, which do not use auto-forwarding, are **not** prohibited. Please refer to the “AUTO-FORWARDING OF E-MAIL POLICY” for additional information.

USPTO RULES OF THE ROAD

- Refer to the “USPTO Tandberg Video Teleconference System Usage Policy” for specific directions on how to prepare for and ensure proper AIS security during video teleconferencing (VTC) operations, with specific attention to the requirements for discussions involving sensitive information.

The following are examples of sensitive data that should not be discussed or transmitted on PTONet or related computing services:

- Anything with sensitive personnel data such as names with Social Security numbers, leave balances, salaries, or benefits for which an employee is signed up.
- Anything dealing with the details surrounding an Employee Relations or Union issue.
- Sensitive procurement information (any procurement in the \$1 million or over category, not purchase orders).
- Anything dealing with the details surrounding contract award prior to an award.
- All information categorized as Source Selection Information by Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423) that concerns the number, identity, ranking, or evaluation of offerors in response to an ongoing procurement action.
- Information marked by an offeror as proprietary.
- Source selection information, including bid prices prior to bid opening, proposed costs/prices in response to a solicitation, source selection plans, technical evaluation of proposals, cost or price evaluations, competitive range determinations, ranking of offers, and reports or evaluations of source selection panels.
- Anything dealing with budget policy prior to the budget submission, particularly as it may deal with USPTO employees.
- Passwords or other computer security related items.

Rule #6: Do not copy or misuse copyrighted material, including software

The use of the PTONet and USPTO AISs, including the ability to access external information through the Internet, offers USPTO users an opportunity to more effectively perform their jobs. This expanded capability also increases the need to emphasize your awareness of copyright restrictions. Many computer programs, and related materials such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Copyright considerations also apply to some of the non-computer related documents that are obtainable through the USPTO’s access to the Internet. Failure to abide by legal and contractual restrictions on the use of copyrighted products could make you subject to civil and criminal prosecution. Therefore, you should observe the following restrictions:

- Copyrighted and licensed materials, including software, should not be used on USPTO AISs or collected or disseminated via PTONet, distributed through the e-mail AIS, or posted in news groups without the copyright or license owner’s approval.

USPTO RULES OF THE ROAD

Rule #7: Do not use PTOnet to harass anyone in any way

The USPTO is proud of its efforts to create a work environment free from all forms of harassment. As a PTOnet and USPTO AIS user, you should not use these resources in any way that unreasonably interferes with anyone's work or creates an atmosphere where others feel harassed. Any USPTO employee who feels harassed should seek assistance and resolution of the complaint. To report on-line harassment, contact the Help Desk at (703) 305-9000.

Assuring Proper Use of PTOnet and USPTO AISs

PTOnet and USPTO AIS resources, as well as news groups, mail servers and Internet resources accessible through PTOnet, are powerful tools that can easily be misused. You should not overload the AIS or otherwise abuse the network.

Rule #8: Do not overload the AIS or abuse the network

In order for the USPTO to obtain maximum use of its PTOnet and USPTO AIS resources, you should carefully evaluate your use of these resources and not overly tax processing and storage capabilities or restrict access by other users. You are encouraged to observe the following:

- Avoid sending e-mail attachments larger than 1 megabyte. This is a document of approximately 30 pages if it is straight text. If graphics or spreadsheets are included, it could be as little as 1 page. See the *USPTO E-Mail User's Guide* for information on sending attachments.
- Do not download voice or video files from the Internet, or stream video or audio data from the Internet, unless approved by your supervisor.
- Archive e-mail messages you need to keep after you have read them. Delete mail you have read but no longer need, and delete old messages and unneeded documents out of file folders.
- Do not send broadcast messages (i.e., messages addressed to a server and/or to all users). Instead use e-mail Shared Folders, or an Intranet "What's New" web page if a message must be widely disseminated.
- Do not attempt to extend AIS processing time by overriding established AIS time limits. Do not automatically forward electronic mail, via rule, macro or script. Automatic forwarding potentially creates a serious operational threat potentially impacting AIS availability. When e-mail is sent to the USPTO mailbox and then forwarded to a destination account, those accounts can reach a maximum size and result in a mail-loop affecting the availability of AISs. The destination account rejects the e-mail due to capacity constraints. The rejection returns to the USPTO account and is again forwarded. The cycle continues, filling the USPTO mailbox with copies of rejected forwarding attempts until detected by USPTO administrators. In the course of this process, the USPTO mailbox can reach hundreds of megabytes in size; far in excess of established maximums.

USPTO RULES OF THE ROAD

- Therefore, auto-forwarding to another destination outside the USPTO network is prohibited. Auto-replies or out-of-office settings, which do not use auto-forwarding, are **not** prohibited. Please refer to the “AUTO-FORWARDING OF E-MAIL POLICY” for additional information.
- Do not develop Scripts, Macros, Web Crawlers, Utilities, Local Applications or other software or batch processes to automate tasks that are run on or are executed against workstations, servers or other network resources other than on your own local workstation. Such development is not permitted without written approval from the OCIO and business executive management for those AISs that the automated process will run and/or execute against. Only OCIO and business executive management is authorized to initiate development efforts to automate tasks that require running and/or executing against the network resource for which they are assigned the responsibility, and in doing this they are required to follow USPTO Life Cycle Management (LCM) processes and documentation procedures. Unauthorized automation of tasks has the potential of adversely impacting AIS availability by significantly impacting the performance and availability of an automated information system (AIS). Solutions to automated tasks need to be designed carefully by authorized persons in accordance with USPTO LCM processes to prevent these occurrences.

Rule #9: Use proper E-mail etiquette

You are authorized and encouraged to communicate with others using the USPTO’s electronic mail (E-mail) service whenever appropriate. The use of e-mail enhances your ability to reach an intended message recipient, saves time, provides enhanced search, retrieval and filing capabilities, and makes electronic records available to many users simultaneously. You are encouraged to observe the following practices:

- Keep your messages as brief and to the point as possible.
- Always fill out the subject line. Give a brief, clear description of the message.
- Identify the author or a point of contact in the body of the message if “FROM” does not have an individual’s name.
- When sending messages to a group, ask yourself “Does everyone in this group need to see this message?”
- Be careful with humorous or witty messages. If sent to people who know you, most likely they will understand your meaning. To strangers, your message may be interpreted as offensive. Assume your message might someday be requested under FOIA or the Privacy Act.
- Your messages should not contain any obscene, profane, discriminatory or otherwise offensive material.
- Some people view upper case as the equivalent of SHOUTING. Be aware of the potential to unintentionally cause offense.

USPTO RULES OF THE ROAD

Remember that once your message is sent, you cannot take it back and it is out of your control. It can be printed or forwarded to others.

Rule #10: Do not compromise the integrity of PTOnet or USPTO AISs

Computer viruses represent a significant threat to the operational readiness of PTOnet and USPTO AISs. Given the USPTO's increasing dependence on the information processed and stored on AISs, it is important that you understand and recognize the basic threat that a computer virus represents. You must learn how to protect against virus infections, detect their presence, and obtain assistance to repair the damage they cause. While there are no easy answers to these problems, you can create a preventive and protective atmosphere by implementing the following safeguards:

- Use only U. S. Government acquired software from factory or officially sealed containers obtained through proper USPTO distribution or requisitioning channels.
- You are prohibited from unauthorized acquisitions, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.
- Public domain freeware or shareware is not authorized for use on USPTO computers without prior testing and approval from the Office of the Chief Information Officer.
- You are prohibited from transferring any software product across the PTOnet, via the USPTO's e-mail AIS or downloading software products from external sources, including the Internet, unless the software has been tested and approved by the Office of the Chief Information Officer.

Rule #11: Protect PTOnet and USPTO AIS assets

The USPTO has invested considerable time and money to establish an automation environment that provides you timely access to the computing resources and information you need. In order to ensure that you continue to receive the service you require, certain actions must be taken to protect USPTO automation assets. You are encouraged to observe the following practices:

- Do not reconfigure USPTO computer hardware and software assets without prior approval. This includes adding privately owned hardware items or software packages to the standard USPTO baseline configurations.
- Do not modify system files without permission of the Chief Information Officer. Modification includes deliberate editing, changing, adding, or deleting of program codes within a system file. This modification restriction does not prohibit you from changing system files as a result of changing desktop parameters, network printer selections, etc., through the desktop operating system environment.
- Do not eat or drink while using USPTO computers. Food crumbs and spilled drinks can cause damage to computer components.

USPTO RULES OF THE ROAD

- Log-off of the PTOnet at the end of your work day and turn off your computer unless specifically requested by the Office of the Chief Information Officer to stay on PTOnet. This helps to safeguard your data by limiting unauthorized access to PTOnet resources and files. Occasionally, you may be asked to leave your computer logged into the PTOnet to facilitate automated software installations and updates. When this occurs, you should turn on the screen saver password feature in the operating system to protect your computer from unauthorized access.
- Never attempt to cut, break or remove any lock or physical security device attached to any Government-owned microcomputer, printer, or other information technology equipment.
- Do not try to perform your own repairs or move your computer to a new location. Call the Help Desk at 305-9000 if your computer is malfunctioning or needs to be moved.
- Do not open any Government-owned microcomputer, printer, or other information technology equipment for any reason. Hardware upgrades must be approved in advance. See the *USPTO Guide to Ordering Computer Equipment* for the approval process.
- Check the placement of your computer, monitor and other electronic computer equipment to make sure that air vents are not blocked or covered. An obstructed flow of air can cause the equipment to overheat and malfunction.
- Prior to and during foreign travel refer to the “USPTO IT Security Handbook” and the “USPTO Information Security Foreign Travel Policy” for specific directions on how to prepare for and ensure proper AIS security.
- It is every USPTO employee’s and contractor employee’s responsibility to report actual or suspected computer incidents and possible virus infections as soon as they occur. You can report all incidents and virus infections to the PTOCIRT (USPTO Computer Incident Response Team) by calling (703) 306-4800 or by e-mail using the “CIRT, USPTO” e-mail address in the Microsoft Outlook Global Address List (you may also use either the CIRT@USPTO.GOV or ABUSE@USPTO.GOV e-mail addresses from within USPTO or from remote locations). Do not send an e-mail to PTOCIRT or anyone else from the infected workstation. PTOCIRT is staffed Monday thru Friday between the hours of 5:30 AM through 6:00 PM. Please leave a voice message with sufficient detail to identify the *nature of the incident and a means to contact you* if PTOCIRT is unable to answer the phone. Computers that are suspected of being infected by a computer virus should be disconnected from the network immediately, remain powered on and attended by someone to prevent others from using the AIS until a *member of PTOCIRT* arrives. AISs should be disconnected from the network by removing the network cable from either the end that is connected to the network interface card (NIC) in the computer or from the end that is plugged into your network wall jack.

USPTO RULES OF THE ROAD

V. RESPONSIBILITIES

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO computer systems, and to employees of contractor systems owned and operated on behalf of the USPTO.

VI. EFFECT ON OTHER POLICIES

This policy affects all new, revised, or retired policies issued in Fiscal Year 2010.

VII. REFERENCES

- *E-Government Act (Public Law 107-347), Title III - Federal Information Security Management Act (FISMA)*, December 2002.
- Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, February 2004.
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, Revised November 2000.
- OMB M-03-22 *Guidance for implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 2006.
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 2006.
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007
- The Privacy Act of 1974, 5 U.S.C. §552a
- U.S. Department of Commerce, *IT Privacy Policy*.
- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005.

USPTO RULES OF THE ROAD

- U.S. Patent and Trademark Office, *Agency Administrative Order 212-4, USPTO IT Security Handbook*.
- U.S. Patent and Trademark Office, *IT Privacy Policy*.
- U.S. Patent and Trademark Office, *Comprehensive Records Schedule*.

ISSUED BY:

John B. Owens II, CIO, USPTO (Signature)


John B. Owens II
Chief Information Officer
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: Office of Organizational Policy and Governance