

Purpose

To define the ES information technology standards of use and to ensure that all use of information technology is consistent with the Northrop Grumman Standards of Business Conduct and Corporate Procedure R1.

Definitions

IIS Internal Information Services

IT Information Technology

Principles

Corporate Procedure CP R1, Computer Systems and Electronic Media, describes acceptable use of Northrop Grumman's information technology services and assigns the responsibilities for the provision of those services to all company elements.

Process

The ES Ethics and Business Conduct Office provides Attachment A175-01, ES Information Technology Use: Management Responsibilities, to implement and ensure that the use of information technology is clearly consistent with the Northrop Grumman Standards of Business Conduct along with Attachment A175-02, ES Information Technology Use: User Responsibilities; Attachment A175-03, ES Web Posting Checklist, and Command Media Form F201-F02, Computer User Security Obligations Agreement.

Evidence

Evidence that this directive is being implemented can take several forms:

- The existence of IT training, communications, and acknowledged Form F201-F02.
- Evidence that a log is maintained of web "pages" created by respective organizations demonstrates that the information is "owned", current, accurate and relevant.
- Evidence that the work on the company information technology resources is authorized by management.
- Evidence that the work being performed is in accordance with the Northrop Grumman Standards of Business Conduct and Corporate Procedure R1 is provided through periodic audits of the above documentation as well as electronic records of receipts and transmissions.

References

Command Media

CP R1, Computer Systems and Electronic Media
CO R102, Inter/Intranet Domain Names

Forms

R201-F02 Computer User Security Obligations Agreement

Other

Commerce Business Daily
Standards of Business Conduct

Attachment A175-01 – ES Information Technology Use: Management Responsibilities

1. Gain an understanding of available IT in order to make business decisions for your organization.
 - Employee Training and Development provides off-hours, simple, short courses.
 - Co-workers, employees and the IT Helpdesk can also provide guidance.
2. Plan your organization's use of the technology.
 - There may be web sites of business interest your staff should check regularly, such as customer-posted information on your program.
 - There may be web sites with free information for which you are currently paying. For example, you can search the current Commerce Business Daily without charge on a number of internet sites.
 - With proper security, you may find the internet and intranet allow for inexpensive and effective sharing of program information with other Northrop Grumman sites, customers and suppliers.
 - You may want to publish ES Intranet web pages to share information within your organization, or to tell others in Northrop Grumman about your organization's purpose and services.
 - You should be aware of web pages established by your organization – whether in general-access areas or password-protected areas. You should ensure your organization is the “owner” of the information and that the information is accurate, current and relevant.
 - You should coordinate web pages within your program, function, division, or discipline to ensure synergy.
3. Authorize business use for people in your organization – including non-employees.
 - Let the people who report to you know your authorization is required for Internet access.
 - All Internet connections are established according to Corporate standards. Internet access is accomplished through the IIS Firewall; exceptions shall be authorized by IIS and Security.
 - You should be aware of use of Northrop Grumman resources by non-employees in your organization and should be cautious of non-US citizens having access to Northrop Grumman systems (refer to item 6 below regarding export controls).
4. Ensure your work force is aware of business use standards.

- During work hours, all IT use, including use of mail services, must be for authorized business purposes only; any off-hours, incidental use must follow procedure on proper use of company resources.
 - Abuse of use privileges may lead to disciplinary action, up to and including termination. Serious disciplinary actions have been taken for misuse. Concerns should be addressed to line management, your HR or Security representative, or the Ethics Office.
 - Illegal, obscene, pornographic, or offensive material must not be accessed, viewed, communicated, or downloaded, such material must not be sent via e-mail. Transmission of such material can result in criminal penalties for individual employees and for Northrop Grumman.
 - Use is subject to audit. ES uses software firewalls to protect against external hacking and to record what sites are viewed, at what time, and by what workstation and user account. Some external sites that have no obvious business value may be blocked from access. Similarly, electronic files are subject to search by company officials.
 - Information published in external usenet groups, such as bulletin boards, must be limited to business related information-gathering requests; users shall share only information that has been approved for public release per Northrop Grumman procedures. Adding a standard disclaimer to a posting disassociating an employee's comments from Northrop Grumman is insufficient and does not protect the Corporation, nor the individual, from legal action.
 - Written approval from the owner shall be obtained before third-party information, such as information owned by suppliers or customers, is published electronically.
 - Copyright law must be followed when publishing any information.
 - All ES information shared publicly on the World Wide Web will be published through the ES external home page and must be approved the Northrop Grumman Communications and conform to Northrop Grumman Procedure CO R102, Inter/Intranet Domain Names. Sites for teamed programs are permitted, as well as participation on customer pages, but any information released via these public pages must be approved by Public Affairs.
 - Provide your work force with copies of the ES Information Technology Use: User Responsibilities; Computer User Security Obligations Agreement; ES Web Posting Checklist; and copies of relevant policies and procedures, as well as explicit guidance.
5. Ensure national security information and foreign government information is properly protected.
- No classified information shall be published or communicated via "unapproved" Internet, Intranet, or e-mail; classified electronic transmissions require endorsed NCI encryption devices and customer approved networks. All automated information systems processing classified information shall be coordinated with the Security Department.

- Unclassified government-owned and customer controlled information requires program management review and Security Department approval prior to electronic transmission.
6. Ensure export-compliance requirements are met.
- Controlled technical data can be published/communicated on ES IT resources only when precautions have been taken to avoid inadvertent export. Providing foreign persons access to export-controlled technical data can be construed as an export. Contact your Contract Representative and/or Export Management for assistance.
 - To avoid inadvertent export, employees on foreign travel shall not access controlled technical data on the ES Intranet without prior approval from Contracts and/or Export Management.
7. Ensure Northrop Grumman systems integrity.
- The Internet is an unsecured network; Northrop Grumman Proprietary, Competition Sensitive, and personal information, shall not be transmitted without appropriate security controls, such as encryption.
 - Downloading information – text or software – must be done per company procedures to ensure viruses do not enter inadvertently, as well as to resolve any software licensing issues.
 - Prior to publishing general information on the ES Web, IIS may be contacted to ensure the server is appropriate for the activity and is adequately protected.
 - All Web pages that need to be secured will be hosted through ES' Intranet server.
 - If the information you plan to post is not something you would publish in your building's main hallway, don't post it in a general-access area of the Internet or the Intranet.

ES Information Technology USE: User Responsibilities – Business Standards for IT Use

While IT resources offer enormous benefits in terms of increased access to information, they also generate a plethora of emerging professional responsibility and legal issues. To achieve maximum performance from our IT resources, as well as to reduce the risk to company assets, IT users are accountable to implement the following appropriate use standards.

1. **Use Company resources for authorized business functions.** It is relatively easy for users to perceive IT resources, such as the internet, as a public resource. Users must remember that Company-owned and government-owned systems are available for authorized work, that is, activities sanctioned by management and position functions. If uncertain about use, ask your manager for specific guidance.
2. **Avoid offensive material.** IT resources provide easy, efficient access to vast quantities of valuable information; however, it can also serve as a conduit for material that could be considered offensive. Access to offensive material cannot be completely filtered without impacting performance and cost. It is therefore the user's responsibility to maintain a professional work environment at all times – immune from harassment, intimidation, and insult.
3. **Respect intellectual property.** The internet was originally established as an academic resource; it was designed to facilitate uninhibited exchange of information. Today it exists in a more diverse and competitive environment. Easy access to information through the Internet begets easy reuse of information derived from Internet sources. Consequently, Internet use increases the risk of copyright violations. Unknowing users expose themselves and the Corporation to liability when electronic information is reused with regard for ownership. Users shall be aware of their legal obligation to recognize and respect the intellectual property of others. Any original work of authorship may be the subject of copyright protection and can only be copied or distributed with the permission of the copyright owner. Such copyright-protected subject matter includes literary text or information, software, and graphic or pictorial works.
4. **Safeguard private and personal information.** Users have responsibility to respect the privacy of others and to safeguard personal information about others that has been entrusted to them for legitimate work purposes. Users shall not access files belonging to another user without permission, nor shall users transmit private or personal information over insecure, public networks. Remember, communications between internal subscribers may remain without network resources; however, messages sent outside Northrop Grumman normally traverse the Internet!
5. **Obtain public release authorization.** Technical information posted to web services requires prepublication authorization. Who authorizes publication depends on the type of information involved. For example, release of information controlled by Department of State export regulations requires authorization from the Contracts Department, while publications pertaining to a Government contract

- probably require customer authorization. Users shall solicit specific prepublication guidance from their local management.
6. **Distinguish opinion from corporate position.** Users expressing opinion on work-related subjects shall obtain management approval and shall attach an explicit disclaimer that states the following: The statement provided is this user's opinion and does not necessarily reflect company position on the subject. Users shall express opinion judiciously and shall refrain from expressing personal opinion on subjects that are not work-related, such as politics, religion, and hobbies.
 7. **Protect information assets.** Competitive advantage and financial success rely heavily on time access to accurate information and protection of sensitive information. While IT use offers enormous advantages, there are significant security issues associated with network communications. Secure system design and other security controls help thwart active outsider threats to computer resources but have minimal affect on unintentional insider threats caused by user errors, accidents, and omissions. Users may unintentionally expose company information systems to malicious intrusion by hackers and viruses as well as other security risks, needlessly impacting performance. Users are responsible for implementing the following security provisions:
 - National Security information is not authorized on any public system; information systems processing classified information require Security Department accreditation prior to use.
 - Proprietary information and intellectual property shall not be transmitted over external networks unprotected; similarly, sensitive information regarding Company products or activities shall not be posed to open environments such as public news groups and bulletin boards, nor discussed via Internet chat sessions.
 - Data, files, and/or software from unknown or suspect sources shall not be downloaded to Company systems.
 - Software that is legitimately downloaded from external sources shall be scanned for malicious code prior to use on any Company system.
 - User passwords shall be protected from disclosure and changed often; non-dictionary words shall be used as passwords.
 - Internet access shall be accomplished through the IIS firewall.
 8. **Enforce CyberEthics.** Users are required to enforce the highest standards of business ethics, regardless of the work environment, and to report known and suspected violations of company policy. Reports shall be directed to local management, your Human Resources or Security representative, or the Ethics Office.

It is the policy of the company to monitor IT use. Similarly, electronic files may be searched by company officials. Individuals violating provisions of Procedure A175 will be disciplined accordingly.

Attachment A175-03 – ES Web Posting Checklist

Answer these questions before posting information on web resources to ensure contractual, security, and other requirements are met.

1. Is the information about an ES program (e.g. commercial programs or government contracts)?

- Yes – go to 2
- No – jump to 4.

2. Is the information controlled by the US Government, NATO, or a foreign government?

- Yes – go to 3
- No – jump to 4

3. Is the information considered by the US Government, NATO, or a foreign government to be classified material?

- Yes – do not post.
- No – go to 4.

4. Does the information have dissemination restrictions under the US State Department International Traffic in Arms Regulations (ITAR) or Commerce Department Export Administration Regulations?

- Yes – information must be protected; jump to 7.
- No – go to 5.

5. Does the information belong to a third party, such as a supplier or subcontractor?

- Yes – information must be protected; jump to 7.
- No – go to 6.
- Unsure – contact the Contracts or Purchasing organization for guidance.

6. Is the information ES proprietary?

- Yes – do not post for all to view. Post in a password-protected mode on the protected Internet server.
- No – go to 7.

7. Should the information be protected by being encrypted?

- Yes – contact the IIS System Integrity for assistance.
- No – go to 8.

8. Should the information be posed in a password-protected mode to restrict viewing?

- Yes – contact ES Webmaster for guidance.
- No – go to 9.

9. Does the information need customer approval, e.g. the System Program Office, before posting?

- Yes or Unsure – contact your Security representative. If customer grants approval, go to 10.
- No – go to 10.

10. Has the ultimate owner of the information , e.g. the program manager, functional owner, macro-process owner, approved publishing on the ES Intranet?

- Yes – go to 11.
- No – acquire approval.

11. Is the information personal (such as biographies or resumes)?

- Yes – post only if approved by your manager. Establish a plan to maintain the currency of the information.
- No – go to 12.

12. Does the server on which the information will reside contain other information that is: (1) proprietary, private, or competition sensitive; or (2) controlled by contractual specification, unclassified Information associated with a government program, foreign government information related to a US Government contract?

- Yes – must use ES' Intranet server for posting these pages to ensure that the sensitive information is protected.
- No – post. Establish a plan to maintain the currency of the information.

