Acceptable Use of the Internet

Guidelines for FSG Sites

FSG

March 1, 2022

Acceptable Use of the Internet

Summary

FSG Sites need to assess the associated risks and publish policies to ensure the appropriate use of FSG systems and networks that provide access to the Internet and technologies used for electronic mail, instant messaging (IM), and peer-to-peer (P2P) file-sharing.

Many users of FSG-owned information resources rely on access to the Internet to perform research to communicating directly with the public. The Internet can encourage collaborative projects and resource sharing; aid technological transfer to businesses; foster innovation and competition; and build a broader infrastructure to support professional, work-related activities. Anyone can abuse the privilege of Internet access, either directly by promoting inappropriate activities and by misusing access time or indirectly by inadvertently allowing unauthorized users to access the network. Internet usage for both personal and professional purposes inherently places FSG information resources at risk. To protect and operate FSG information resources properly, all stakeholders must have policies that consider the following:

- Security: Protect all data stored or transmitted on FSG resources
- Liability: Avoid downloading illegal, copyrighted and/or unauthorized content
- Compliance: Manage bandwidth usage, personal time and costs, and records retention

FSG sites must ensure that computers and the important information they store and transmit remain secure, private, and protected. Each FSG site retains the flexibility to develop the most appropriate means of accomplishing this goal through a combination of sound management policies and effective technological means.

Recommendations

All FSG sites that have not published a policy on Peer-to-Peer file-sharing should initiate actions by August 1, 2018, to publish a policy. The policy must include clearly defined provisions for permitted use, restrictions, and enforcement.

All FSG sites should consider implementing one or more of the technological measures to control unauthorized P2P and other Internet activity based on the associated risks.

Managing Risk through Policy and Technology

All FSG sites should develop practical and enforceable policies regarding acceptable use of the Internet including e-mail, IM, and P2P technologies. Acceptable use policies should take into account requirements for security, liability, and compliance. Each of these areas is explored in more detail below. The example policy statements included in the appendixes contain some statements that may apply to some FSG sites, but not others. The specific
wording in the example policy statements is, in most instances, purposefully general in nature, allowing management to assume responsibility for defining acceptable practices and exercise full judgement according to their own specific risk assessments.

FSG sites may choose to have users acknowledge their acceptable use policies in writing, e.g., as part of their initial check in or account creation process. Additional online options for user access policy acknowledgement include banners as part of the user log-on, customized portal applications, Local applications, policy awareness and other tools, policy management, applications, and Windows domain authentication.

Useful features for these user awareness applications include compliance tracking (tracking access, personal statements and testing), easy access and Web interface searching, an alerting mechanism to warn users about new threats, templates to facilitate policy creation and updates, and management links to external standards.

Whether acknowledgement is written or electronic, user access policies should consider the following factor:

- FSG policies should forewarn network users that all Internet activity via FSG networks or computers is subject to monitoring. Whenever a user accesses the Internet via a FSG information resource, all activity may be logged and can be used to detect or confirm a user who conducts illegal or unauthorized activity.

Internet monitoring is both a management and a technical issue. The use of FSG information technology resources is a privilege. If an authorized user fails to comply with this policy or relevant laws, that user's privilege to access and use FSG information technology resources may be revoked. Users typically access the Internet through one more of the following channels:

- **Web browsers** are software applications that can locate and display Web pages (Firefox and Internet Explorer are the most common); most can display graphics, text, and multimedia, including sound and video.

- **E-mail** is short for electronic mail, the transmission of messages over communications networks that usually have gateways to other computer systems via an Internet Service Provider (ISP).

- **Instant messaging** provides real-time textual communications between individuals using proprietary Internet protocols.

- **Peer-to-peer** file-sharing programs are Internet applications that allow computer users to share electronic files with other users connected to a common file sharing network. P2P represents over 60% of all Internet traffic by data volume, and that figure is growing (see CacheLogic 2004 P2P Traffic Study).