9.3. Using The Internet

Objective

9.3.1. Personnel use Internet services in a responsible and security conscious manner, consistent with agency policies.

Context

Scope

9.3.2. This section covers information relating to personnel using Internet services such as the Web, Web-based email, news feeds, subscriptions and other services. Whilst this section does not address Internet services such as IM, IRC, IPT and video conferencing, agencies need to remain aware that unless applications using these communications methods are evaluated and approved by GCSB they are NOT approved for communicating classified information over the Internet.

9.3.3. Additional information on using applications that can be used with the Internet can be found in Section 14.3 - Web Applications and Section 15.1 - Email Applications.

Rationale & Controls

Using the Internet

9.3.4.R.01. **Rationale**

Agencies will need to determine what constitutes suspicious activity, questioning or contact in relation to their own work environment. Suspicious activity, questioning or contact may relate to the work duties of personnel or the specifics of projects being undertaken by personnel within the agency.

9.3.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1529]

Agencies MUST ensure personnel are instructed to report any suspicious activity, questioning or contact when using the Internet, to an ITSM.

Awareness of Web usage policies

9.3.5.R.01. **Rationale**

Users MUST be familiar with and formally acknowledge agency Web usage policies for system users in order to follow the policy and guidance.

9.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1532]

Agencies MUST make their system users aware of the agency's Web usage policies.

9.3.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1533]

Personnel MUST formally acknowledge and accept agency Web usage policies.

Monitoring Web usage

9.3.6.R.01. **Rationale**

Agencies may choose to monitor compliance with aspects of Web usage policies, such as access attempts to blocked websites, pornographic and gambling websites, as well as compiling a list of system users that excessively download and/or upload data without an obvious or known legitimate business requirement.

9.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1536]

Agencies SHOULD implement measures to monitor their personnel, visitor and contractor compliance with their Web usage policies.

Posting information on the Web

9.3.7.R.01. **Rationale**

Personnel need to take special care not to accidentally post information on the Web, especially in forums and blogs. Even Official Information or UNCLASSIFIED information that appears to be benign in isolation could, in aggregate, have a considerable security impact on the agency, government sector or wider government.

9.3.7.R.02. **Rationale**

To ensure that personal opinions of agency personnel are not interpreted as official policy or associated with an agency, personnel will need to maintain separate professional and personal accounts when using websites, especially when using online social networks.

9.3.7.R.03. **Rationale**

Accessing personal accounts from an agency's systems is discouraged.

9.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1541]

Agencies MUST ensure personnel are instructed to take special care when posting information on the Web.

9.3.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1542]

Agencies MUST ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites.

9.3.7.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1543]

Agencies SHOULD monitor websites where personnel post information and if necessary remove or request the removal of any inappropriate information.

9.3.7.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1544]

Accessing personal accounts from agency systems SHOULD be discouraged.

Posting personal information on the Web

9.3.8.R.01. **Rationale**

Personnel need to be aware that any personal interest or other information they post on websites can be used to develop a detailed profile of their families, lifestyle, interest and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit information from them or implant malicious software on systems by inducing them to, for instance, open emails or visit websites with malicious content.

9.3.8.R.02. **Rationale**

Profiling is a common marketing and targeting technique facilitated by the internet.

9.3.8.R.03. **Rationale**

Individuals who work for high-interest agencies, who hold security clearances or who are involved in high-profile projects are of particular interest to profilers, cyber criminals and other users of this information.

9.3.8.R.04. **Rationale**

The following is of particular interest to profilers:

- photographs;
- past and present employment details;
- personal details, including DOB, family members, birthdays, address and contact details;
- schools and institutions;
- clubs, hobbies and interests;
- educational qualifications;
- current work duties;
- details of work colleagues and associates; and
- work contact details.

9.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1550]

Agencies SHOULD ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.

9.3.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1551]

Personnel SHOULD be encouraged to use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.

9.3.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1552]

Personnel SHOULD be encouraged to undertake a Web search of themselves to determine what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.

Peer-to-peer applications

9.3.9.R.01. **Rationale**

Personnel using peer-to-peer file sharing applications are often unaware of the extent of files that are being shared from their workstation. In most cases peer-to-peer file sharing applications will scan workstations for common file types and share them automatically for sharing or public consumption. Examples of peer-to-peer file sharing applications include Shareaza, KaZaA, Ares, Limewire, eMule and uTorrent.

9.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1555]

Agencies SHOULD NOT allow personnel to use peer-to-peer applications over the Internet.

Receiving files via the Internet

9.3.10.R.01. **Rationale**

When personnel receive files via peer-to-peer file sharing, IM or IRC applications they are often bypassing security mechanisms put in place by the agency to detect and quarantine malicious code. Personnel should be encouraged to send files via established methods such as email, to ensure they are appropriately scanned for malicious code.

9.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1558]

Agencies SHOULD NOT allow personnel to receive files via peer-to-peer, IM or IRC applications.