

Summary of proposed changes in IT Security Policy (rev 1.14)

Section I

1.15/2.6 Drive sanitization before disposal

Remove DoD 5220 M, cite NIST SP800-88. Remove mention of licensed s/w.

3 Scanning language enhanced

Committee: regular scanning of the whole network

7.a Guest Wireless

Change to accommodate new open guest Wi-Fi

Section II

2 Expiring border firewall exceptions

Committee: annual or per-rule expiration

Section V (new)

New section on cloud security

Summary: OK to use the cloud for default/public data

Restricted data requires approved contract OR VPIT OK

No Private data in the Cloud without approved contract AND VPIT OK

General cleanup/definitions/typos

Other security committee recommendations

IAC security subcommittee recommends elevated scanning across the board and firewall rule expiry as immediate policy changes, to be implemented as resources allow. The committee also discussed a number of procedural recommendations, as well as some longer-term system projects, and wanted to express the security benefit posed by several other ongoing efforts. None of the non-policy recommendations are presented for discussion or voting today, and none seem to belong in policy language; they are presented as a more comprehensive response to the committee's charge to make recommendations to shore up our security posture.

Procedural/management

- Enhanced firewall request process (web form, more info, stored registration, may trigger scan)
- Maintain list of supported server OS/apps/protocols (like desktop & network versions, arrow up/side/down)
- Investigate systematization of dev/admin training
- Review security staffing in light of other recommendations

Longer-term system acquisition/development

- Training/cert/skills tracking software (buy [SkillSoft] or develop in Canvas; run in HR or OTD?)
- Data Loss Prevention/PII scanning
- Application-aware firewall functions & IDS/IDP for datacenter

Support for other initiatives/committees

- Accelerate Slate adoption for graduate applications
- Transition plan from eID WebAuth to Shibboleth (with 2FA and Social auth)
- 2FA for privileged access to central data
- Clarify accepted uses of CSUID and eID