# Information Security Checklist

Esther Silver on January 28, 2020

## Policy Type

Best Practice

1. POLICY: Have you read and understood UCSF Network and Information Security policies and related procedures? - Review policy 650-16 [1] - Information Security and Confidentiality
2. CONFIDENTIALITY AGREEMENTS: Has the execution of properly signed confidentiality agreements been verified before proprietary and/or sensitive information is disclosed, in any form, to individuals outside the organization?
3. PHYSICAL SECURITY: Are buildings, paper records, and sensitive IT resources within them (e.g., computer and network equipment, storage media, wiring closets) properly secured from unauthorized access, tampering, damage, and/or theft by an intruder with malicious intent?
4. BUSINESS RESUMPTION PLAN: Does the organization have a documented and frequently tested business resumption plan for critical computer system and associated office support infrastructure that includes frequent system backups, off-site data backup storage, emergency notification, replacement IT and office resources, alternate facilities, and detailed recovery procedures?
5. ANTI-VIRUS: Are all computer systems protected with up-to-date anti-virus software and other defenses against malicious software attacks?
6. INTERNET SECURITY: Are all dedicated connections to the Internet and other external networks properly documented, authorized, and protected by firewalls, intrusion detection systems, virtual private networks (or other forms of encrypted communication), and incident response capability?
7. REMOTE ACCESS: Are modem and wireless access point connections known, authorized, and properly secured?

8. PASSWORDS: Have all vendor-supplied, default passwords or similar "published" access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products been changed or disabled?
9. SOFTWARE PATCHES: Are security-sensitive software patches, including the removal of unnecessary sample application software, promptly applied to systems that are accessible to users outside of the organization?
10. DATA PROTECTION: Is sensitive, valuable information properly protected from unauthorized access, including Windows network file shares and undocumented (desktop) web and FTP servers?
11. AUDITS AND VULNERABILITY TESTING: Are all computers and network devices (e.g., routers and switches) within your organization regularly tested for exploitable vulnerabilities and unauthorized (or illegally copied!) software?

A negative or unsure response to one or more of the above questions places an organization in a position of unnecessary risk, not only to heightened possibility of direct financial loss and/or public embarrassment by a security incident, but also the loss of confidence and credibility in the organization. For further assistance, please contact ITS Customer Support [2].



---



**Links**
[1] http://policies.ucsf.edu/policy/650-16
[2] http://help.ucsf.edu/