HARVARD
Information Security

Harvard University Information Security Policy:
Requirements For All Level 5 Environments
Version 0.8: DRAFT as of March 20, 2014

Scope: All servers and applications storing, processing, or providing access to Level 5 confidential information (both Harvard and vendor operated) and all operational processes supporting the management of Level 5 data.

Data Classification Levels: 5

Audience: Anyone who participates in the management of Level 5 data including managers of Level 5 facilities as well as operators and administrators of Level 5 servers.

Note 1: *Because Level 5 environments present a unique set of challenges, a complete set of requirements are presented here.*

Note 2*: The University CISO or his/her designee must certify that the proposed implementation meets Level 5 Requirements.*

Section 1 – Physical Security Requirements

1.1. Confidential information repositories (including servers) must be stored and used only in one or more physically secure rooms. The secure rooms do not have to be dedicated to a specific Level 5 project.

1.2. All entry points to the room(s) must be controlled. Exits must be controlled or alarmed.

1.3. The interior of the room should not be visible from outside the building if the room is located on the ground floor.

1.4. A facility may be certified to house Level 5 systems and data.

Section 2 - Access Security Requirements

2.1. The IRB, if appropriate, and University CISO or his/her designee must be provided with a list of the individuals who will be permitted to have unescorted physical access to the room(s). Other visitors to the secure area are only permitted in special circumstances (e.g., health emergencies, IT support & security reviews). Such visitors must be escorted at all times and their actions must be monitored.

2.2. Individual physical access to the secure area must be controlled and logged.

2.3. The log of physical access must be protected and restricted from unauthorized access.

2.4. The room(s) must be off the janitor's key and must be off the general building master and sub master keys.

Section 3 - Network Security Requirements

3.1. The IRB, if appropriate, and University CISO or his/her designee must be provided with written justification if a Level 5 system is to be connected to a network.

3.2. Any network connected to Level 5 systems must be localized and must not extend outside the secured room(s). If there are multiple rooms, network connections between rooms must be protected by electrical conduit unless the rooms are adjacent.

3.3. No system on a network that connects to Level 5 systems may be accessible from outside the secure room(s) by any means.

3.4. No wireless network capability can be enabled on any Level 5 system.

3.5. No remote access capability can be enabled on any Level 5 system.

Section 4 - System Security Requirements

4.1. Level 5 systems should be dedicated to the single purpose of processing or storing the Level 5 information.

4.2. Level 5 systems must not be removed from the secure room(s) unless any storage disks in the system have properly cleaned by making the Level 5 information unretrievable.

4.3. All administrative functions on the Level 5 systems or applications that access Level 5 information must be logged. The logs should include the identity of the user, the time and the command executed.

4.4. Logs recording administrative functions on Level 5 servers should be reviewed frequently to determine if the systems are under attack and that the users are following the documented access practices (e.g., not logging in as root).

4.5 Level 5 systems connected to any network must run host-based firewalls configured to block all connections to the system other than the specific connections needed to perform the approved research tasks.

4.6 Documented practices must be in place on maintaining the configurations of the host-based firewalls.

4.7. Generic accounts on systems must be disabled.

4.8. Default passwords on systems must be changed before systems are put into use.

4.9. A mechanism must be in use on systems to inhibit attackers guessing passwords (e.g., lockout after multiple bad password guesses).

4.10. A mechanism must be in use on computers to block access to idle sessions (e.g., an application timeout or a locking screen saver).

Section 5 - Operational Security Requirements

5.1. People responsible for the operation of servers must have the skills, experience and/or training needed to implement these requirements.

5.2. A server operator must be able to identify a responsible party for each application on the server.

5.3. There must be a written list of the individuals or the categories of people (e.g., research assistant, lab administrator) that are permitted to have accounts on the Level 5 systems ("The access policy") or otherwise have access to the data on portable media; the names or categories must be disclosed to the IRB, if appropriate, and University CISO or his/her designee.

5.4. Users must only have access to the confidential information through their individually assigned (non-shared) user accounts.

5.5. Only the applications that are actually required to support the services used in connection with the Level 5 data can be running on the servers.

5.6. Servers must enforce Harvard standard password complexity rules. (See http://www.security.harvard.edu/resources/best-practices/passwords.)

5.7. Confidential information taken out of the Level 5 server, in whatever form/way it may be (e.g. over a network, on portable storage, etc.), must be encrypted.

5.8. All portable media (including magnetic media such as portable disk or thumb drives and non-magnetic media such as optical disks or paper) containing Level 5 information must be encrypted or locked in a safe, which is in a physically secure room, when not actually in use.

5.9. All portable media (including non-magnetic media) containing Level 5 information must not be removed from the secure room unless the removal has been specifically approved and logged.

5.10. Servers and the applications must be designed so that passwords cannot be retrieved by anyone (including system administrators). (This should include a mechanism to ensure that any assigned passwords are changed on initial use.)

5.11. Interactive access to servers must be logged. The logs should include the identity of the user, the time and the function (login or logout).

5.12. Users' access to Level 5 data or servers must be removed if they no longer have a reason under the access policy to access the information (e.g., they change jobs or leave the university).

5.13. There must be a documented practice to ensure that any actual or suspected breach is promptly reported to IRB and the OGC, as well as the University CISO, the School CIO, and the University CIO.

5.14. Level 5 information is not permitted to be stored on any user computer or portable computing device (e.g. laptop, PDA, or smartphone). (See note below about collecting Level 5 information)

5.15. Backup tapes containing Level 5 information must be encrypted.

5.16. All electronic records containing Level 5 information must be properly disposed of by overwriting the information or physically destroying the media.

5.17. Unused or broken disk storage drives that were used to store Level 5 information must be properly disposed of by overwriting the information or physically destroying the media.

5.18. The IRB, if appropriate, and University CISO or his/her designee must approve any plans to have a vendor store or process the Level 5 information.

5.19. Contracts must be executed with all external vendors who process or store Level 5 information at Harvard's direction.

5.20. The contracts must contain specific contract language (approved by the OGC) that requires the vendor to protect confidential information and to inform Harvard promptly of any possible breach that may put the information at risk of exposure.

5.21. The contracts must contain specific language (approved by the OGC) to ensure that Level 5 information is not stored on a user computer at a vendor.

5.22. The contracts must contain specific contract language (approved by the OGC) to ensure that the protection of the Level 5 information meets the requirements in this policy.

5.23. Harvard employees working with Level 5 information must annually acknowledge a confidentiality agreement and be appropriately trained.

5.24. Implementation of operational requirements is subject to review and audit by the IRB, if appropriate, CISO, RMAS, and/or other appropriate authority.

Section 6 - Field Collection Security Requirements

Collection of Level 5 information while in the field must adhere to strict security protocols. The protocol(s) to be used must be approved by the IRB and University CISO or his/her designee.

Some examples include:

- Computer based collection of Level 5 information in the field may only be done by saving the collected information to an encrypted disk or an encrypted thumb drive with an appropriate password or passphrase.
- The information should be transferred to a secure server as soon as practical.
- The Level 5 information must remain encrypted until it is on a Level 5 system.
- The Level 5 information must be promptly and properly erased (i.e. overwritten) from the computer or media used to collect the Level 5 information once the transfer has been completed and verified.