System Security Plan
University of Texas Health Science Center
School of Public Health

Note: This is simply a template for a NIH System Security Plan. You will need to complete, or add content, to many of the sections depending on your specific project with NIH. We have highlighted all the instruction areas in yellow. Please review each section carefully and contact SPH IT Services for any additional details.

1. Information System Name/Title

[Enter the name of the system (or systems)]

2. Information System Owner

[Enter the name and contact information for the system owner]

Derek Drawhorn
Asst Dean, Information Technology Services
University of Texas Health Science Center Houston
School of Public Health
1200 Herman Pressler
Suite RAS E-17
Houston, TX 77030
(713) 500-9533
Derek.d.drawhorn@uth.tmc.edu

3. Other Designated Contacts, Including Those with "root" Access.

[Enter the names and contact information for any other critical technical or administrative contacts for this system. This should include the IT (policy) director, system administrators, data center contacts, etc]

Chris Harvey
Asst Director, Information Technology Services
University of Texas Health Science Center Houston
School of Public Health

1200 Herman Pressler
Suite RAS E-17
Houston, TX 77030
(713) 500-9544
Christopher.m.harvey@uth.tmc.edu

4. Assignment of Security Responsibility

[Who is responsible for implementing security policy? Enter the name and contact information of the security contact for this system, if different from above]

Information security is a multi-tiered approach from both the systems administrators *(listed above)* in cooperation with the UTHSC Information Security team. The contact below is responsible for securing enterprise level systems, while the systems administrators are responsible for the physical and logical security of the system.

Amar Yousif
Information Security Officer (ISO)
University of Texas Health Science Center Houston
7000 Fannin, Suite UCT M-50F
Houston, TX 77030
(713) 486-2227
Amar.Yousif@uth.tmc.edu

5. General System Description/Purpose

[Please describe the system and its purpose. Is this a standalone system, a compute farm, shared use system, desktop PC? What is the operating system, version? What is the data storage capacity?]

6. Physical System Environment

[Where is this system maintained? Data Center, Lab? What physical access controls exist to secure the system? For example, is there a defined list of people

with physical access to the system? Access record keeping system? Locking system? Alarm systems? Video surveillance?]

Describe specific system.

If your system involves the use of DESKTOPS, please include this section below…

All desktops are running the Windows 7 or Windows 8.1 operating system and are fully patched as of the submission of this document. All desktops are full-disk encrypted using Windows Bitlocker encryption technology. All desktops are members of the University domain and are enrolled in a number of security policies and systems, including:

- Automated application and operating system patch management using Microsoft Systems Center Configuration Manager. All operating system patches are tested and pushed within 48-96 hours of release.
- Automated virus/malware patch management using System Center Endpoint Protection. Virus definitions and engine updates are automated and installed daily, even before there is public knowledge of a given patch release.
- Domain Group Policy Objects. All desktop computers must comply with University GPO's including screen saver timeouts and strong password enforcement.
- Desktop Firewall. While the University maintains a complex and robust enterprise firewall for the network, all desktops additionally have a software firewall implemented to further restrict incoming requests for service or data. This software firewall is maintained by the contacts listed in this document.

If your system involves the use of SERVERS, please include this section below…

All servers at SPH are housed in a secure data center. Characteristics of these protections provided are:

- Physically secured environment where the location is provided on a need-to-know basis.
- A tiered firewall strategy must be deployed to provide both extranet (Zone20), internet (Zone40), and protected (Zone100) servers. Each zone becomes increasingly more secure and better protected from each lesser zone. Each

server must be identified and registered into a specific zone and give appropriate and documented privileges from the IT Security Department to operate in its zone and traverse between any other zones.

- Access controls deployed which account for who can access the rooms, logged and routinely audited access control logs, 24 hour video surveillance of the entire facility, and policy for the escort of visitor in/out of the facility.
- Environmental controls for all server environments to include: Building independent temperature/humidity controlled environment fully supported by emergency power, perimeter walls extending from the structural floor to structural ceiling, access control lists must be maintained so that only authorized personnel are permitted access to data center and other sensitive areas, the access control list must be reviewed semi-annually by the data center owner or their designate to ensure appropriate access, evidence of review and resulting modifications to the list must be maintained by a period of time as designated by Records Management policy of the University, access logs must contain the names of persons, date and times visitors enter and leave the facility, all entry and exits must be monitored via video surveillance. All activity should be electronically stored for future reference as required.
- Additional physical security features include:
    - Self closing and locked access doors
    - Remotely monitored security alarms
    - Uninterruptible Power Supply (UPS) adequate to supply 100% of system power for a 15 minute duration
    - Fire detection and suppression system
- Data Backup. A documented plan must be created, implemented and tested to allow data recovery in the event of data corruption or data loss. It is the resource owner's responsibility to keep the plan current as the computing resources and technology change over time. The resource owner may delegate this responsibility to the steward or system administrator of record but accountability remains with the resource owner.
- Data Storage. Resource owners must secure all confidential and sensitive data in the GRA. Physical access to data storage areas must be limited to authorized personnel. Storage area access should be secured by a card reader and/or written logs containing user name, date and time of entry. Written logs may contain the reason for visit (optional, but recommended).
- Offsite Data Storage. Offsite storage of sensitive, confidential and University proprietary data is permitted by an approved vendor utilizing environmental

and secure access controls specific to the type of data stored at offsite storage facilities.

- Media Disposal. All media currently having or having in the past contained confidential or sensitive information must be securely destroyed. Methods for destroying media could include degaussing, physical shredding; Department of Defense approved data removal techniques, or other methods of physical destruction. Wherever possible, a full accounting of all drives and tapes that have been physically destroyed should be obtained by the vendor providing that service. Any additional support documentation, such as a video surveillance of the disposal session, is highly recommended.
- Media Accountability. All media containing confidential, sensitive and proprietary data must be clearly labeled when not in use and stored in a secure area that is restricted to personnel with a verifiable need to access this area. Sensitive documentation, such as data printouts, faxes, and other document formats containing software license information or similar, should be stored in a secure location when not in use, preferably in a lockable filing cabinet or desk.
- Controlled Media Access Lists and Logs. All media containing personal healthcare information (PHI) data must be stored in a secured area.
- Disaster Recovery Plan. A detailed disaster recovery plan must be created for identified systems to restore records and service in the event of server destruction. The plan must be updated and tested as documented in the disaster recovery plan.

If you would like to request a copy of the actual "Physical Security Policy" (UTHSC ITPOL-10), please contact the System Owner as identified in Section 2. These policies are available by request only as they can pertain confidential information which might expose the University if made publicly available.

7. System/Network Diagram

[Insert a diagram of the relevant portions of the systems to convey system and network architecture. Please include relevant off-site links, data storage locations, user-access points and firewall locations.]

The University network is divided into "zones" which identify their specific layer of protection and degree of separation from the internet. These zones are:

- Zone 0 – Internet
- Zone 20 – Extranet or DMZ
- Zone 40 – Intranet
- Zone 100 – Protected

Each zone is protected by redundant enterprise grade firewalls. Each zone is designed to provide additional protections from attack or industry vulnerability as you move up within the zone infrastructure. Below is a summary of where certain devices typically reside within the zoning infrastructure.

- Zone 0 – Internet - Very few devices live in this zone. This zone is only available in one data center on campus and highly regulated by University Network Operations and Information Security. All servers in this zone must have logging and auditing turned on and these logs are reviewed using real time threat analysis techniques.
- Zone 20 – Extranet or DMZ – Only public-facing servers, typically web servers, reside in this zone. All servers in this zone must have audit logging software installed and all events are reviewed using real time threat analysis techniques. No workstations live in this zone and this zone is only accessible from University sponsored data centers. Firewall restrictions are in place to prevent access from Zone 20 into Zones 40 and 100 without specific permissions.
- Zone 40 – Intranet – This zone is reserved for desktops and general purpose servers. This zone is generally available throughout the campus, but servers in this zone are required to reside in a University sponsored data center. Firewall restrictions are in place to prevent access from Zone 20 into Zones 40 and 100 without specific permissions.
- Zone 100 – Protected – This is the most protected and monitored zone. All servers with confidential or protected information reside in this zone. Systems residing in this zone are typically database and file servers. All servers in this zone must have audit logging software installed and all events are reviewed using real time threat analysis techniques. No workstations live in this zone and this zone is only accessible from University sponsored data centers. Firewall restrictions are in place to prevent access from Zone 20 into Zones 40 and 100 without specific permissions.

If you would like to review any of the three existing policies which affect system and network diagramming, please contact the System Owner as identified in

Section 2. These policies are available by request only as they can pertain confidential information which might expose the University if made publicly available. These policies are:

- Network Configuration Policy (ITPOL-008)
- Network Security Policy (ITPOL-009)
- Firewall Security Zone Policy (ITPOL-003)

8. System Interconnections/Information Sharing

The University has numerous policies and guidance which impact System Interconnections and Information Sharing. If you would like to review any of the nine existing policies, please contact the System Owner as identified in Section 2. These policies are available by request only as they can pertain confidential information which might expose the University if made publicly available. These policies are:

- Password Policy (ITPOL-002)
- Portable Storage Device Policy (ITPOL-001)
- Laptop Security Policy (ITPOL-007)
- Host Configuration Policy (ITPOL-006)
- Acceptable Encryption Policy (ITPOL-003)
- Access Control Policy (ITPOL-004)
- Change Management Policy (ITPOL-005)
- Information Resources User Acknowledgement Form (ITF-001)
- Contractor Confidentiality Acknowledgement Form (ITF-002)

8.1. Security Controls

[What security controls are in place to protect the data and system? What encryption will be used for data stored on portable devices or laptops? How are security patches and updates applied?]

By policy all data must be stored on protected systems. All file services and databases are stored on servers residing in Zone 100, our most protected zone. When data is in transit, whether on a laptop or portable media, the data must be encrypted as well – no exceptions. All laptops must deploy full disk encryption

using Windows BitLocker or another product in compliance with the University's acceptable encryption policy.

All servers and desktops, no matter the location or manufacturer, are required to be enrolled in an automated patch management system. Servers and desktops are primarily managed using Microsoft Systems Center Configuration Manager technology which includes automated patch management, automated application distribution, and extensive reporting. As a validation measure, IT Security uses a separate product, QualysGuard, to validate patch installations and compliance on a quarterly basis. Working together, the University provides exceptional independent validation of configurations and patch compliance.

8.2. Access Control

[How is access control implemented to restrict access to these data to those authorized and how are data protected from being copied to unapproved locations? What protections are in place to identify, authenticate and control external user access?]

There is no unauthorized access allowed to any system. Local guest or admin accounts are strictly prevented by policy and routinely audited by desktop managers. All systems, including database applications, are required to have authenticated and permission based roles for access. Generic access to all system and resources is highly discouraged.

At this present time, there is no copy protection which would prevent an authorized person from copying this data to any other source, internal or external. However, the Access Control Policy governs access to all systems which prohibits the unauthorized copying of data to non-protected systems. Additionally, automated safeguards are in place with IT Security which scan outbound traffic identifying and notifying IT Security when certain types of confidential data leave the network. This would include protected health information, social security information, and payment card industry information. IT Security has full time network analysts who monitor these logs in real time responding to alerts as they arise.

All external users are required to obtain a "guest account" for any access to any system. A guest must have a faculty sponsor, must provide identity information

to the sponsor for account request, the guest must appear in person and provide validated proof of their identity to an independent reviewer. Guest accounts can only be granted for up to one year and the renewal process is similar to the original process, in that both the sponsor and the guest must confirm the renewal of the guest account.

8.3. Awareness and Training

[What is the process to ensure all users have had the necessary computer systems security training and acknowledge the sensitivity of access to these data?]

All new employees are exposed to a one hour information security training session before being given access to their credentials. The University IT Security team additionally provides electronic information via their website and mail messages regarding security policy and acceptable use issues. A link to their awareness website is included below.

IT Security Awareness website - http://its.uth.tmc.edu/aware_home.htm

Starting in 2009, every employee is required to complete an online security and awareness training seminar. This information is compiled by IT Security each year and every employee must satisfactorily pass an online exam to complete the training. Aside from information technology awareness training, each employee is also required to complete training and exam regarding the protection of confidential data.

8.4. Configuration Management

[As system configurations change, what tracking is in place to ensure that security is maintained?]

The University has a well established change management system (ITPOL-005 Change Management) for all security and enterprise wide changes. The individuals referenced in this document are responsible for configuration and change management. Additionally, a virtual boundary exists between the University IT Security department and the Network Operations department. This level of separation provide a greater level of oversight into network security since both teams independently review each group.

8.5. Auditing and Accountability

[How are IT infrastructure and security audited? How frequently? Are audit records maintained and protected?]

Auditing of information technology systems is a multi-tiered approach. There are annual audits conducted by the University of Texas System. These audit are conducted by independent contractors and vary from year to year based on security incidents from the previous year. These audits have been related to hardening of systems in accordance with national regulations such as HIPAA, PCI, and Sarbanes-Oxley.

Locally, auditing of systems is conducted by the Office of Institutional Compliance which is a non-IT entity employing attorneys with technology emphasis to conduct security audits throughout the year. Each year, based on a local assessment with top IT personnel, audits are conducted for compliance and security activities. These reports are provided to the President of the University and then rolled up to the University of Texas System.

With the University IT Security department, they conduct credentialed quarterly scans of all servers in all zones for security and compliance matters. As well, desktop zone scans are conducted on a more routine basis. The University has employed two full time network security analysts whose job it is to watch and oversee real time data movement issues throughout the system, looking for and taking action on any anomalies occurring.