CITY UNIVERSITY OF HONG KONG
Network and Platform Security Standard

(Approved by the Information Strategy and Governance Committee in January 2023)

INTERNAL **Date of Issue: 2023-01-28**

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-08-25	Typo corrections
1.2	2023-01-28	Revised the link and reference material in this document. Added Web Application Firewall (WAF) in 6.2 Web server

Distribution

Copy	Issued to	Location
Master	Public	https://www.cityu.edu.hk/cio/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

The City University of Hong Kong ("University") must maintain secure network infrastructure and platforms, including network equipment and hosts, by implementing appropriate security controls to protect the University's IT environment, and review security level of its IT environment regularly and as necessary.

2 Objective

This document provides the minimal requirements and process for protecting the University's network infrastructure and information processing platform.

3 Network Infrastructure

The University maintains a complex network structure to supports its activities and enable communications, in forms of data, voice and video. The network is the first line of defense against malicious activities.

3.1 Network Segregation

To simplify control, network of computing resources are grouped and segregated into security zones by location, function, and classification of information being processed. The depth or number of zone layers should commensurate to the sensitive of information being processed.

The network zone defines the boundaries and security defense requirements.

Appropriate network security equipment, such as Network and Application Firewall, Reverse Proxy, Intrusion Detection System ("IDS"), Intrusion Prevention System ("IPS"), and etc., should be installed to protect the computing resources in the isolated zones.

Cross-boundary network traffics (depicted as white arrows in Figure 1) must be channeled through the network security equipment.

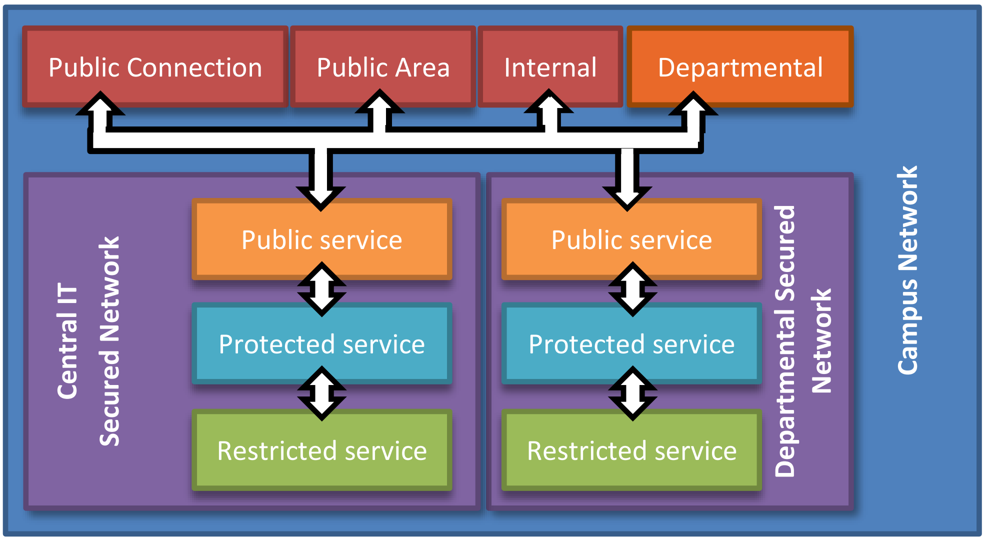

Figure 1) Network Security Zones in the University

3.2 Public Connection Networks (Untrusted)

The University maintains Public Connection Network in form of Wireless Networks, Virtual Private Networks ("VPN"), Wired Guest Network and Student Hostel Network that are accessible to the public.

Some University's Units also maintain Departmental Student Local Area Networks ("LAN") and Laboratory Networks.

The users within these networks use their own devices. Computing resources in these untrusted networks are not controlled nor managed by the University.

Traffics from these untrusted networks shall be handled the same way as Internet traffics.

3.3 Campus Public Area Network (Untrusted)

Computing resources in Campus Public Area Network are managed by the University, and shared among the active members of the University. Examples are the student terminal area and the express terminals setup in the campus area, as well as PC clients in library public area, library catalog terminals.

Though the computers in this public area networks are managed by the University, however, administrator privileges are usually granted to the users. Users may install virtually any applications to these computers during their session of use. Hence, traffics from this public area networks should be handled the same way as traffics from the Internet.

3.4 Internal Network (Untrusted)

Some University Units manage their own networks within Campus Network for dedicated purpose. Examples of these networks are Networks in

- Off-shore Campus, Remote Office and Branch Office
- Private Control Network and Smartlock Network of CDFO
- Departmental Internal Networks and Laboratory Networks

Unless designed, managed, assessed, and monitored by qualified security professionals, these networks are classified as Untrusted.

3.5 Departmental Network (Managed)

Departmental networks are centrally managed by CSC and are only accessible to staff, appropriate contractors and third party users. Computers in these networks are usually assigned to designated users, or only shared among a small group of users.

Computing resources in these networks are used to process “**INTERNAL**”, “**CONFIDENTIAL**” as well as “**RESTRICTED**” information of the University.

However, “**CONFIDENTIAL**” and “**RESTRICTED**” information should be removed from these networks once processing is completed.

Computers and network equipment in these networks shall be hardened and regularly assessed to ensure the appropriateness of configurations.

3.6 Secured Network (Trusted)

“**CONFIDENTIAL**” and “**RESTRICTED**” information should be kept in protected storage servers inside the secured networks and transmitted to Internal Network or Departmental Network only when necessary. Depending on functions and security requirements, the secured networks could further be segregated into inner zones. For typical 3-tier web applications, the secured network should be segregated into:

- Public service network - for presentation tier which handles interactions between applications and end-users. This inner zone may provide limited accessibility to the public in order to provide necessary services, however, no information should be stored in this servers in this zone. Any information in this zone must be transient.
- Protected service network - for business tier which process data. This segment should only be accessible to the public service sub-network.
- Restricted service network - for persistence tier in which the file servers or database servers are installed. This segment should only be accessible to the restricted service sub-network.

Computers and network equipment in these networks shall be hardened and regularly assessed to ensure the appropriateness of configurations.

4 Internet Gateways and External Gateways

The University’s Campus Network (“CTNET”) is managed by CSC. Any other networks are external networks to the University.

- Internet gateways connect the University’s network to the Internet.
- External gateways directly join the University’s network to network of partners, such as networks of subsidiaries and overseas branches of the University, the other Universities, and third party service providers. Examples of interconnecting networks that require external gateways are private leased lines, Multiprotocol Label Switching (“MPLS”) and Virtual Private Networks (“VPN”).

CSC is responsible for managing and monitoring of Internet gateways, which hooks the University up to the Internet. CSC is also responsible for managing and monitoring external gateways which provide service to all members of the University.

University's Units shall not arrange their own Internet gateway and external gateway, unless prior registration and approval from CSC is obtained. CSC shall establish registration and approval procedure to handle application for gateways owned and managed by University Units. All access to the Internet or external networks must be channeled through registered and approved gateways.

The gateway owners or controllers must ensure that proper security measures are implemented to protect the University's network from security threats. Proper security measures must also be implemented to detect and defense against attacks.

As the University's network bandwidth is a limited resource, exceptionally high use of this resource has an impact on all other users. CSC shall monitor the network usage and ensure the fair use of the University's network bandwidth. CSC shall also establish guidelines on network bandwidth usage, and procedure to monitor, notify, warn and suspend machine having exceptionally high network bandwidth usage.

All gateways that are connected to the CTNET and providing access to the Internet and external networks must provide the following security functions:

- Firewall for access control
- Packet-filtering routers for routing traffic and packet filtering
- Protection against computer virus
- Intrusion detection system (IDS) and monitoring system for attack detection

Unregistered gateways are recognized as illegal backdoors. All University Units shall report their installed Internet gateways, external gateways, and externally allocated IP address ranges to CSC on a yearly basis or as requested by CSC. CSC shall reconcile the reported gateways and IP address ranges with the registry to identify illegal backdoors. All illegal backdoors must be disconnected from the University's networking immediately when found.

CSC should confine the network segments and devices connecting directly to the illegal backdoor, and disable network activities of these segments and devices until security assessment is completed with satisfaction results.

5 Network Security

The owners or controllers of networks must deploy appropriate security components to protect the network zones and the information resources in the zones, including but not limited to the following:

- Firewall
- Demilitarized Zone (DMZ)
- Network Address Translation (NAT)
- Network Access Control
- Virtual LAN (VLAN)
- Virtual Private Network (VPN)
- Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS)
- Anti-malware
- Proxy and Reverse Proxy
- Logging and Log monitoring
- Network QoS/Traffic Shaper
- Pseudo air gap or air wall

Figure 2 illustrates a sample logical network infrastructure with recommended security components.

Connections between networks; and installation, modification of configuration; and removal of equipment must not compromise or downgrade the security level of network zones. All network equipment must be properly configured.

The owners or controllers of networks shall classify and document their network infrastructure and submit these documents to Central IT for recording purpose, and make these documents available to Central IT when requested.

Network infrastructure must be reviewed and endorsed by qualified security professionals recognized by Central IT prior to implementation and after major changes. Changes in network infrastructure must be submitted to Central IT for recording purpose within 1 month after implementation.

Configuration of all equipment on the network, including firewalls, routers, hosts and etc., must be hardened according to security baseline configuration published by the University.

Owner or controller of network must designate specific individuals for equipment configurations. Privileges to modify configurations of equipment must only be granted to the delegated individuals.

Network security devices, such as firewall and router, shall be implemented to separate “untrusted”, “managed” and “trusted” networks. Network security devices must also be implemented to separate the University’s networks and external networks

Firewall and router rule sets shall be reviewed by qualified security professional at least every 24 months, or after significant changes of network infrastructure.

Restrict inbound and outbound traffic across network zones are necessary for the zones’ data environment and data usage.

All traffics across trusted zones shall be denied by default; permissible traffics shall be explicitly allowed and documented with justification.

All traffics across external networks, including the Internet and partner networks, shall be denied by default; permissible traffics shall be explicitly allowed and documented with justification.

Transmission of sensitive information outside secured network and managed networks must be encrypted.

Private IP address shall be used with system components in trusted zones. Private IP address shall not be disclosed to unauthorized parties.

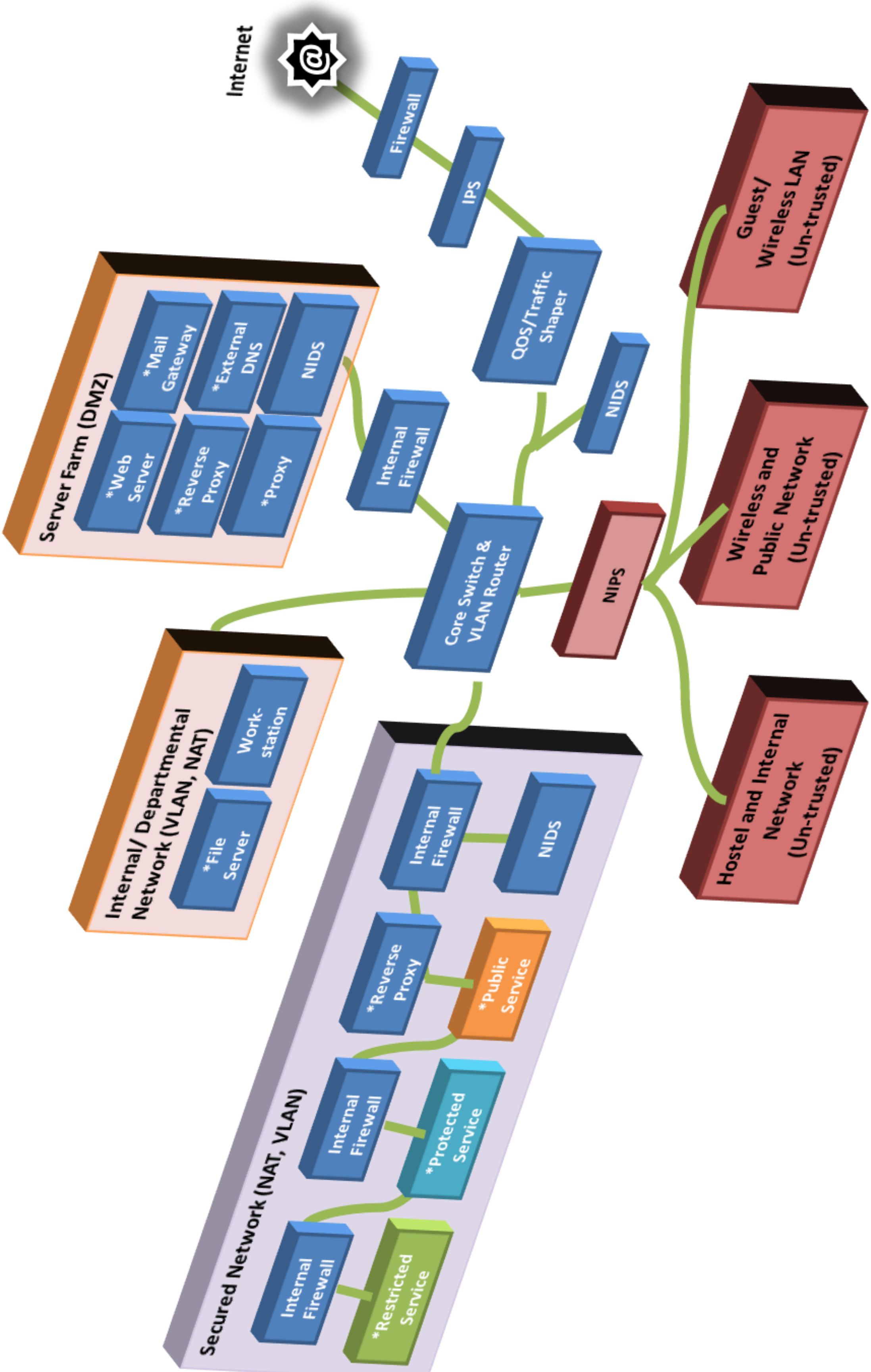

Figure 2) Logical network infrastructure with security protection

6 Host Platform Security

A Host Platform is a foundation or base, which consists of hardware (such as tower and blade servers, virtualization infrastructure, and networked/attached storage) and software (such as operating systems, databases and application servers). To prevent functions (e.g. web server, database, etc.) that require different security levels conflict or interfere with each other, only one primary function should be implemented on each host.

6.1 Operating System ("OS")

There are often vulnerabilities in OS. Security patches for OS shall be applied. The owners or controllers of the host platforms must ensure that all the host platforms are protected by appropriate security controls.

All OS running desktop or server in managed network and trusted networks must be configured and hardened according to the host configuration baseline of the University.

The owners or controllers of OS shall ensure that appropriate security measures are implemented to protect their OS, such as:

- Anti-malware, including anti-virus and anti-spyware with subscription to vendor supplied definitions and automatic update enabled; enable regular scans if appropriate.
- Patch management system or auto update for installation of security patches, within one month of release
- Authorization and authentication of all users
- Audit trail and event logging
- Host based firewall, and configured appropriately
- Host Intrusion Detection System ("HIDS") and Host Intrusion Prevention System ("HIPS")
- Disk or file system level encryption
- Restrictive and secure file access permission and control
- Resource isolations, such as isolating the disk partition of user directories and OS directories, and limiting the CPU and memory resources available by process

6.2 Web Server

Web server is usually the "front-most" server visible to the end-users, and exposed to the Internet. Web servers are first target of both manual and automatic attacks; therefore, strong host and network security protection should be implemented.

The owners or controllers of web servers shall ensure that appropriate security measures are implemented to protect their web servers, such as:

- Web directories shall not be on system disk, such as "%SYSTEMROOT%" of Windows
- Use virtual "jail" environment to confine the access of web server
- Follow the principle of least-privileged user account ("LUA"), such that web service must be able to access only information and resources necessary to its function, e.g. start web services using account that does not have write access to web directories
- Prevent "path traversal" by implementing appropriate controls, such as server-side input validation, URL rewrite and jails.

- Turning off server-side executable codes
- Use HIDS and/or HIPS to detect and/or prevent intrusion
- Review content in web directories to remove outdated materials
- Remove or disable default accounts, unused account
- remove sample contents from vendor
- limit web server from reporting platform and version information to queries
- Disable unnecessary protocols, such as WebDAV
- Restrict access to administrative interface to managed network or trusted network
- Implement Web Application Firewall (WAF) to protect public-facing web application / application programming interface (API) by filtering, monitoring, and blocking any malicious traffic

6.3 Application Server

Application servers host customized web applications, and interactive with end-users. Numerous malicious attacks are targeting application servers, and the custom application or services deployed to application servers.

The owners or controllers of OS shall ensure that appropriate security measures are implemented to protect their web servers, such as:

- Application directories and work directories shall not be on system disk, such as “%SYSTEMROOT%” of Windows
- Use virtual “jail” environment to confine the access of application server
- Follow the principle of least-privileged user account (“LUA”), such that web service must be able to access only information and resources necessary to its function, e.g. start web services using account that does not have write access to web directories
- Limit application server from reporting platform and version information to queries
- Disable unused services and connectors
- User Reverse Proxy to prevent end-user from directly connecting to applications servers
- Use SSL to protect data transmission
- Applications and services must be reviewed for security vulnerabilities prior to deploy to application servers (Refer to “Software Development Standard (Under construction)”)
- Disable client side stack tracing or debug report if any
- Restrict access to administrative interface to managed network or trusted network
- Disable automatic application deployment
- Restrict access to application server binaries (executable), configuration, log, temp, and application directories
- Disable remote sample applications and guest accounts
- Enforce connection timeout and idle timeout

6.4 Database and Content Repository Server

Database servers and content repositories provide persistence service for storing important information asset of University. The confidentiality, integrity and availability are of the utmost concern.

The owners or controllers of database servers and content servers shall ensure that appropriate measures are implemented, such as:

- Deploy server in a trusted network, behind a firewall to reduce remote attack service
- Disallow direct access to server from Internet or untrusted networks
- Disallow the server from creating direct outbound access to Internet or untrusted networks
- Use a least-privileged account for data or content repository service
- Enable and use database encryption service if available
- Enable and use table and column encryption service if available
- Use a non-default port to protect database from attacks directed to default port numbers
- Rename user name of administrator account
- Use separation partitions for OS, Database or Content repository program, data file, audit trail, transaction logs, and etc.
- Use separated and dedicated directories for program, data file, audit trail, transaction logs, and etc.
- Set service to auto start and auto restart
- Database user accounts and content repository accounts shall be created following the principle of least-privileged user account
- Disable anonymous or guest accounts
- Grant “executes” permissions on stored procedures to database user roles instead of individual user accounts directly
- Do not assign “grant” option to database users or roles
- Enable audit trail and regularly review audit logs to identify any attempted security breach

6.5 Virtualization platform

Virtualization platform is the foundation of many computing systems. The owners or controllers of virtualization platforms shall ensure that appropriate security measures are implemented to protect their platforms, such as:

- Virtualization infrastructure shall be deployed in a trusted network, behind a firewall and disable inbound from all networks except trusted network for infrastructure management, and outbound traffic to all networks except website of vendor for security patches and updates
- Access to virtualization platform from guest systems shall be disabled

7 Configuration Baseline

Configuration baselines are documents that specify the hardening requirements of IT products to the target operational environment. IT products are any vendor-supplied IT products, including but not limited:

- Hardware, such as computer hardware, network printer, and etc.
- Software, such as operating system (Windows, Solaris, etc.), application server, database system, and etc.
- Network equipment, such as firewall, NIDS, NIPS, router, load balancer and etc.

The Information Security Unit ("ISU") and Computer Service Centre ("CSC") are responsible for purposing and publishing configuration baselines of the University, based on industry-accepted system benchmarks, including but not limited to the following sources:

- Center for Internet Security ("CIS")
- National Institute of Standards Technology ("NIST")
- SysAdmin Audit Network Security ("SANS") Institute

ISU and CSC are also responsible for regularly review and adopt the University's configuration baselines to change in environments and new needs raised.

The configurations of IT products must be hardened before installing or enabling the IT products on the production network. The owner or controller of the product shall modify the configurations by following:

i. the configuration baseline of the University
ii. if (i) above is not available, use the vendor-supplied benchmark or benchmarks from CIS, NIST, or SANS
iii. if (i) or (ii) are not, source an industry benchmark or best-practice, and notify ISU of the selected benchmark

There are situation that the suggested settings in the baselines or benchmarks may negatively inhibit the utility or performance of the product and conflict with the function required by the owner. In cases when an exclusion of setting found to be avoided, the exclusion needs to be justified and evidence is needed to proof the necessity of the exclusion. The ISU should be notified for any exclusion of settings.

8 Continuous Security Assessment

The owners or controllers of network infrastructures and computing platforms are responsible for conducting continuous security assessments to ensure that security controls required in this document are implemented appropriately and security level of their networks and platforms are maintained.

Continuous security assessment shall be conducted on IT environments regularly or after implementation of major changes, or as required by the ISU or CSC.

Prior to implementation of major changes, security review and risk assessment of changes should be conducted.

Continuous security assessment is recommended to be performed at least once a year for critical systems.

Both continuous security assessment and security review shall be conducted by qualified security engineers in the University or by qualified external service providers recognized by the University.

ISU and CSC are authorized to conduct security assessment on any IT components on the University's network to ensure that these components do not impair the security level of the University's IT environment.

The owners or controllers are responsible for managing or mitigating the risks found during security assessments.

9 Summary

The University must ensure sufficient security measures are implemented to ensure that the network infrastructure and computing platform are protected from security threats, and attacks are effectively monitored and defensed. The University must also ensure that the security level of its IT environment is maintained, by conducting regular security assessment.

References

The following documents were consulted during the preparation of this document:

Center for Internet Security (2020), *CIS Apache HTTP Server 2.4 Benchmark*, v2.0.0

Center for Internet Security (2022), *Security Configuration Benchmark for Apache Tomcat 10 Server Benchmark*, v1.0.0

Center for Internet Security (2022), *CIS Microsoft Windows Server 2022*, v1.0.0

Center for Internet Security (2020), *CIS Oracle Database Server 19c*, v1.0.0

Office of the Government Chief Information Officer, Government of Hong Kong (2022), *IT Security Guidelines*, Version: 9.1

Appendix A

Sample “Scope of Work” for Security Assessment. Owners or controllers shall prepare the scope of work appropriate to their IT environment.

Scope of Work

1.1. *Security Assessment Service Providers*, as IT Security Assessor (“assessor”), in responsible for the evaluating the technical security level against industry benchmarks and best practices.

1.2. *Owner Department*, as System Owner (“owner”), owns the Information System to be evaluated in the IT security assessment.

1.3. The Information System (“system”) includes *Internet visible systems for information sharing (i.e. systems managed by owner and accessible from the Internet)*, the data processed by these components and systems, and the direct related IT infrastructure components (i.e. network and servers). The following systems will be evaluated in this assessment:

1.3.1. *Campus Network infrastructure*
1.3.2. *HTTP servers*
1.3.3. *FTP servers*
1.3.4. *SharedPoint servers*
1.3.5. *Web Application servers*

1.4. The assessor shall perform a security assessment to the network infrastructure and security controls in network to propose recommendations for improvements.

1.5. The assessor shall perform vulnerability scanning and penetration testing which should cover the following where appropriate:

1.5.1. *Network level probing/scanning and discovery*
1.5.2. *Host vulnerability tests and discovery*
1.5.3. *System/application scanning*
1.5.4. *Black-box Web application vulnerability scanning*
1.5.5. *Secure code review on custom Web applications for SANS TOP-25 and OWASP web application vulnerabilities*

1.6. The assessor shall prepare a vulnerability scanning and penetration testing report detailing the tests conducted and the results upon completion of the tests. Before conducting the tests, the owner should agree with the assessor on the possible impact and fallback/recovery procedure.

1.7. The assessor shall perform risk analysis on the following aspects:

1.7.1. Physical security
1.7.2. Access control security
1.7.3. Data security
1.7.4. System Security
1.7.5. Application Security
1.7.6. Network and communication security

1.8. The assets and their associated risk will be evaluated through the following process:

1.8.1. Asset identification and valuation
1.8.2. Threat analysis
1.8.3. Vulnerability analysis
1.8.4. Asset/threat/vulnerability mapping

1.8.5. Impact and likelihood assessment

1.8.6. Risk results analysis

1.9. Based on result of risk analysis, the assessor shall recommend appropriate security controls to reduce the likelihood and impact of identified risk to an acceptable level

1.10. The assessor and the owner shall ensure that the security assessments have minimum impacts on the daily operation of the system. All activities must be carefully scheduled to avoid/minimize service interruption