IBTS Policies

Following elements must be in place and managed properly, the consent of higher management shall be present in order to represent the seriousness of the overall security posture of the broker owning IBTS.

IT Security Program

The program includes the development of policies, procedures, and guidance that define minimal acceptable security practices to standardize IBTS's approach to security. The program ensures a coordinated defense of the IT resources. This involves implementing centralized security resources to provide an umbrella of protection for all systems (such as access control, security training, intrusion detection, and incident response capabilities). In addition, it involves a formal authorization process for each IBTS system and routine periodic security evaluations. This includes verifying that the level of security is appropriate for each system and implementing corrections for identified weaknesses.

Establishing an Appropriate Level of Security

1. Security shall be applied to IBTS IT resources using a risk-based approach.
2. Non mitigated vulnerabilities are documented in the system security plan and the risk formally accepted
3. Security must be commensurate with the sensitivity level of the system and take into account existing threats, vulnerabilities, and value of the asset.
4. All information resources are assigned a sensitivity level rating (e.g. low, medium, or high)
5. Sensitivity levels are determined by the resource owners with respect to the confidentiality, integrity, and availability requirements of the data processed by and/or stored within the system and are documented in system security plans.
6. These sensitivity levels are used within IBTS issue-specific policy to satisfy security requirements and to prioritize security reviews.

In order to establish an appropriate level of security, following elements of the security program must be properly governed:

Security Reviews and Penetration Testing

1. All IBTS systems must undergo an independent security review, as per Internet Trading Regulations
2. IBTS Systems may undergo additional periodic technical security reviews and pen-test as determined by events (e.g., vulnerability notifications and security incidents), system changes, and changes to the system sensitivity levels.

Interconnected Systems

Some IBTS systems have direct connections to other IT systems through the use of dedicated lines, virtual private networks, or some other connection such that the security levels of the systems affect each other. This often happens when two distinct networks are joined together.

This can also happen when two or more entities need to collaborate on a project by sharing resources. Since a trust relationship exists between the two systems, vulnerability in one system could create a security exposure in the other system. In these cases:

1. The IBTS system owners must ensure that the interconnected systems have commensurate\ levels of security.
2. The IBTS Owner must approve all interconnections with other systems and may require that an interconnection agreement be established between those organizations.
3. IBTS Owner may also need to review the design and architecture of such engagement to ensure technical feasibility and authorize the same.

Jointly Owned Systems

It is not always possible to assign an IT resource to only one system. In some cases, the hardware and operating system is maintained by one department (e.g., systems department) while the software and user access controls are maintained by Development Department. In these cases:

1. Both departments will jointly own the IT resource, and
2. System owners will apply security controls to their respective domains and ensure that the controls are properly integrated.

Security Incident Investigation and Reporting

All IBTS related incidents, including suspicious, malicious, and illegal IT activity must be reported to the Exchange.

Nonpublic Information

1. IBTS Owners must implement measures to protect nonpublic information from disclosure

Such as:

a. Include the issue of disclosure of nonpublic information as part of the risk assessment.
b. Have all employees who have access to nonpublic information sign non-disclosure
c. Review access controls periodically.

2. IBTS Owners must establish and document the safeguards against disclosure of nonpublic

3. IBTS Owners must have a documented framework for applying appropriate access controls, based on data criticality and sensitivity. Also, when data are shared with other departments, the regulators, or federal agencies, those data elements should be classified at the higher level of data criticality, as determined by the departments involved.

Information Security Controls

Following security controls must be in place to protect information resources of the IBTS by its Owner and custodian.

Access Control

The following shall apply to IBTS and all critical systems associated to it, including those containing nonpublic information:

1. Must have documented procedures for creating, managing, and rescinding user accounts.

Minimally, the procedures should address:

A. Eligibility criteria for getting accounts.

B. Processes for creating and managing accounts including:

I. Process for obtaining user agreements regarding the campus' Acceptable User Policy.

II. Process for managing the retention of records.

2. Must implement authentication and authorization processes that uniquely identify all users and appropriately control access to systems.

A. Prohibit group or shared IDs, unless they are documented as "Functional IDs." Functional IDs are user accounts associated with a group or role that may be used by multiple individuals or user accounts that are associated with production job processes. Establish procedures for identifying and retiring group or shared IDs.

B. Follow strong password characteristics and management practices, requiring users to adhere to organizational usage, construction, and change requirements. The following password characteristics and management practices are recommended:

I. The user must select and/or change initial passwords, unless those passwords are randomly generated.

II. Passwords must contain a minimum of eight characters.

III. When a user password is reset or redistributed, the identity of the user must be validated.

Considering the heterogeneous computing environments, the following password characteristics and management practices are recommended, but are operationally dependent:

I. Initial passwords and password resets distributed to the user must be issued pre-expired, forcing the user to change the password upon logon.

II. Passwords must contain a mix of alphanumeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters.

III. Passwords must not contain leading or trailing blanks.

IV. Automated controls must ensure that passwords are changed at least as frequently as every 90 days for high-privilege users and every 180 days for general users.

V. User IDs associated with a password must be disabled for a period of time after not more than six consecutive failed login attempts, while allowing a minimum of a 10-minute automatic reset of the account, for critical administrative systems containing non-public information.

To determine password parameters, construction rules and authentication protocols, perform the following:

I. Conduct a risk assessment for authentication of the information system. The risk analysis measures the severity of potential harm and the likelihood of occurrence of adverse impacts to the system, if there is an error in identity authentication.
II. Map identified risks to the applicable assurance level. After all of the risks have been identified, IBTS owner should tie the potential impact of the risks to the proper level of authentication to be implemented.
The required level of authentication assurance should be determined, based on the potential impacts of an authentication error on:
I. Inconvenience, distress, or damage to standing or reputation
II. Financial loss or liability
III. Harm to the organization or public interests
IV. Unauthorized release of sensitive information
V. Civil or criminal violations

Define four levels of authentication, assurance for electronic transactions and identifies the criteria for determining the level of electronic authentication assurance required for specific applications and transactions. These criteria are based on risks and their likelihood of occurrence. As the consequences of an authentication error and misuse of

credentials become more serious, the required level of assurance increases: Level 1 is the lowest assurance, and Level 4 is the highest. The levels are determined by the degree of confidence needed in the process used to establish identity and in the proper use of the established credentials.
Level 1 — Little or no confidence in the asserted identity's validity
Level 2 — Some confidence in the asserted identity's validity
Level 3 — High confidence in the asserted identity's validity
Level 4 — Very high confidence in the asserted identity's validity
Once a level of authentication assurance has been established, password parameters, Construction rules and authentication protocols should be utilized that correspond with the requirements, depending on the level of authentication assurance identified.

C. Implement and document processes to ensure that access rights reflect employee status, including changes in employee status. For critical systems, employees' access rights may be modified, as appropriate, by the close of business on the same day.

D. Implement and document processes for periodically (at least annually) verifying employees' access privileges. It shall include privileges for software, and systems accessing critical data /resources.

3. IBTS (and all of its individual / related components, if any) shall maintain appropriate audit trails of events and actions related to critical applications and data. Furthermore, the following mentioned significant actions and events must be documented and reviewed on consistent basis:
I. Additions and changes to critical applications.
II. Actions performed by highly privileged users (including users defined software use).
III. Additions and changes to users' access control profiles.
IV. Direct modifications to critical data outside the application.

4. IBTS owners must ensure that all critical systems have the ability to log and report specific security incidents and all attempted violations of system(s) security. In addition, there shall be a document processes for reviewing IT security violations on a daily basis.

5. Must segregate the functions of system administration, programming, processing, or authorizing business transactions, and duties, providing for the appropriate separation of security and administration.

Controls for Connectivity Devices

Remote connectivity

There shall exist, a well-documented process for approving and managing the dial-in-access; remote connectivity via ISDN, VPN, Internet, Metronet or Radio. Following security controls shall be in place before the deployment of such systems.

1. There shall exist a well-defined Access control criteria.
2. Detailed access log shall be maintained.
3. Appropriate security controls for remote access services should be put in place.
4. Protecting critical data in-transit (e.g., encryption).
5. It is the responsibility of connecting parties with VPN privileges to ensure that unauthorized users are not allowed to access internal networks.
6. Remote connectivity shall be authenticated, preferably by using a one-time password such as a token device.
7. When actively connected to the corporate network, VPN shall force all traffic directed to and from the Client PC (or network) over the VPN tunnel, mainly includes business applications only. All other traffic shall be dropped to enter in this tunnel.
8. Any software for VPN probes or other such tools shall not be used for any reason.

9. Users of computers that are not IBTS owned equipment must configure the equipment to comply with VPN and Network policies of IBTS Owners. IBTS Owners shall enforce its compliances
10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of network provided by the IBTS Owner, and as such are subject to the same rules and regulations that apply to IBTS owned equipment.
11. Any user found to have violated this policy may be subject to disconnection in the form of service unavailability for an unspecified time frame. However any other misuse may reflect a legal action against the offender according to the state law, or in the Exchange regulations.

Network Devices

1. Network switches and routers (including firewalls, content switches, IDS etc.) should have well defined access controls.
2. All network devices (e.g., servers, routers) should have all non-needed services disabled and the security for those devices hardened.
3. All devices must have updates and patches installed on a timely basis to correct significant security flaws.
4. Default and initial passwords should be changed upon installation of any device /equipment.

5. Implement ingress and egress filtering at the edge of the institution’s network to prevent various network attacks.
6. The responsible network administrator must determine the timeframe for applying security patches and updates based on such factors as risk, inter-dependence, and criticality of service. This process should be very well documented.
7. Central configuration management is recommended for Network devices such as router or switches to avoid any inconsistencies in the network.
8. Administrative activities of all network equipment e.g. change logs etc. shall be maintained well documented, and shall duly comply with the configuration management policy.
9. To verify effective controls on network devices, the IBTS owner shall benchmark these devices in a security review according to appropriate controls and industry best practices.
10. All connectivity Logs shall be maintained at a central place, this shall include logs of the devices as well as user connectivity.
11. Access logs and detailed configuration shall be reviewed.

Security devices
Firewalls

1. The IBTS network must be protected by firewalls at identified points of interface as determined by system sensitivity and data classification.
2. Firewalls should be configured to block all services not required and disable unused ports, hide and prevent direct accessing of trusted network addresses from non-trusted networks, and maintain comprehensive audit trails. Consider establishing dedicated platforms for firewalls.
3. Firewalls should have all non-needed services disabled and the security for those devices hardened. All devices must have updates and patches installed on a timely basis to correct significant security flaws.

Anti-Virus, DLP and other Malware Protection Mechanism
1. All computers connecting from any location must use the most up-to-date anti-virus software of a corporate standard.
2. Signatures and patches should be updated, at least on daily basis.
3. Configuration Change of such system should be very well-documented and exception logs shall be sent to a central logging system.

Server/Services Controls

Following shall be applicable with regard to server systems:

1. Servers systems should not have any non-needed software installed. An inventory of application software per server role shall be maintained.
2. Servers systems should be configured for intended services only, for servers with multiple services, multiple conditions apply, and these conditions shall be detailed as special security controls.
3. System hardening processes for server systems should be well documented.
4. Administrator accounts or any other user accounts should be restricted on per user basis.
5. Unused code and executable should be removed from the application servers.
6. All administrative access should be logged, along with system and application errors/warning; exceptions be sent to central logging system.
7. Physical access to server/services should be well defined and documented.
8. Appropriate Configuration Management shall be implemented.

Central Logs Management

Logs management pertains to effective and intelligent use of logs. Logs management also includes log validation and log archiving system and log retention procedures. Access to logs should be very well defined; the access restrictions and privileges depend on the type of log. For example security logs are viewed by Administrators only, while

System and application logs are also viewed by development department, for error checking of applications.

Criteria for the log management are given below:

1. Logs should be retained for at least five years. The time of log retention depends on regulatory requirements and possible use of logs as evidence at a later time.
2. There should be a defined chain of command for the custody and handling of logs in logical and physical formats.
3. Logs should be effective and usable.
4. Extensive logging should be enabled on all information systems.
5. Some automated alerting mechanism shall be used to trigger alerts.

Security Monitoring

This activity can be part of a periodic security review, or day to day monitoring of critical information assets of the IBTS for potential security incidents.

1. Technical and operational security controls must be periodically monitored to ensure the continued security of the system.

2. The amount and details of monitoring should commensurate with the sensitivity level of the system.
3. Monitoring must only be performed by individuals with security responsibilities and only within the system(s) for which they are responsible. These personal shall work transparently with IT security function, and report critical anomalies directly to the IBTS owner, and later to the Exchange.
4. A log of all monitoring activities shall be maintained, in temper proof logging system.

Segregation of Duties

1. Duties must be separated among multiple employees whenever necessary and possible to prevent a single person from performing malicious or illegal activities undetected.
2. When it is not possible to implement segregation of duties, compensatory controls must be established.
3. Segregated duties and related compensatory controls must be documented within system security plans.
4. All administrative controls shall be well documented by each department along with their detailed SOPs. Security controls custodian dept. (network, system etc.) of IT shall document all related technical controls in these regards.

Configuration Management

Configuration Management adheres to all configuration management of all the servers and clients' software and hardware. Configuration management can be done by centralized software or hardware or by manually configuring devices/software. Following shall be implemented:

1. There should be an electronic centralized configuration management system for IBTS.
2. There should be a defined process by which audits or security reviewers can determine the usability and effectiveness of configuration management so tware or process.