Amman Stock Exchange
Internet Trading - IT Controls

Control	Control Existence	Management Approval	Periodic Review	Comp.?	Comments
Information Security Policy The company should develop an information security policy that should cover the following:					
• Data management and classification					
• Physical and environment security					
• Internet and intranet security					
• Email security					
• Communication and operations management					
• Logical access controls					
• Acquisition, development and maintenance of information systems					
• Periodic review of information security policy					
Confidentiality Requirements All employees shall sign a confidentiality agreement with their respective companies					
• Confidentiality agreement					
• Annual review of the agreements by the company's management					
• More strict provisions in the agreement for employees serving in critical positions					
System Vendors Vendors access to companies' information system shall be provided based on a formal contract					
• Signing system vendors agreements					
• Agreements shall contain confidentiality and non-disclosure clauses					
• Term of service					

Physical and Environmental Security Physical access to information processing areas and their supporting infrastructure should be controlled					
• Secure Data Center (servers and communication equipment)					
• Limited access					
• Authorized access					
• Access logged					
• Firefighting equipment					
• UPS and generators if possible					
• Maintenance agreements for Data Center equipments					
• Labeling all equipment and cables					
Operational Procedures and Responsibilities Companies should develop an operational procedures manual that documents all its critical processes and all changes to information systems environment shall be documented					
• Operational procedures manual includes: ✓ Applications ✓ Hardware specifications ✓ Operating systems ✓ Database configuration ✓ Network configuration					
• Document, review, authorize, and test changes in operational manual					

Password Management (for customers and employees) All information systems shall require identification and authentication through passwords.					
• Passwords authorization, creation, communication procedures					
• All systems must be password protected					
• Minimum passwords length six characters					
• Passwords should be alphanumeric					
• Stored passwords in Databases should be encrypted					
• Default passwords should be changed					
• Unused accounts should be removed					
• User accounts lock after three failure attempts to login					
• Users' credentials reset procedure after lock					
• Session inactivity handling procedure					
Monitoring Significant event details in information systems shall be logged and reviewed					
• Logging significant events for: ✓ Application ✓ Database ✓ OS ✓ Hardware					
• Review logs periodically					

Information Backup and Media Handling All applications, databases, user configuration, and hardware configuration shall be back upped in accordance with backup and restoration procedures. Media shall be controlled and physically protected					
• Backup should include databases, applications, operating systems, hardware configuration: ✓ Backup schedules and procedures ✓ Backup restore procedures ✓ OS mirroring					
• Labeling backup media					
• Backup media should be stored in safe and secure environment					
• Backup copies with documented restoration procedure should be stored in remote locations					
Network Access Control and Configuration Management The following policies shall be complied with during configuration of the companies' firewalls					
• Internal network must be segregated from the ASE network using firewalls and ACLs. Back office must be located in the DMZ					
• Firewall should be placed between DMZ and internal networks					
• All protocols ports and services allowed should be documented					
• Disable unnecessary and insecure services and protocols					
• Review firewall logs periodically					
• Installation of the latest security patches					

World Wide Web Companies WWW resources shall be secured					
• Secure online trading application servers under firewalls' DMZ					
• Applications and Databases vulnerabilities assessment (by the ASE)					
Protection against Viruses					
• Installing Antivirus applications that is constantly updated with the latest virus definitions released					
Securing Customer Transactions Companies should implement adequate cryptographic techniques to secure transactions transit					
• Strong encryption protocols for transmissions of transactions					
Contingency Plans The company should develop a contingency plan pertaining to the Internet trading process					
• Contingency Plan for Internet trading service					