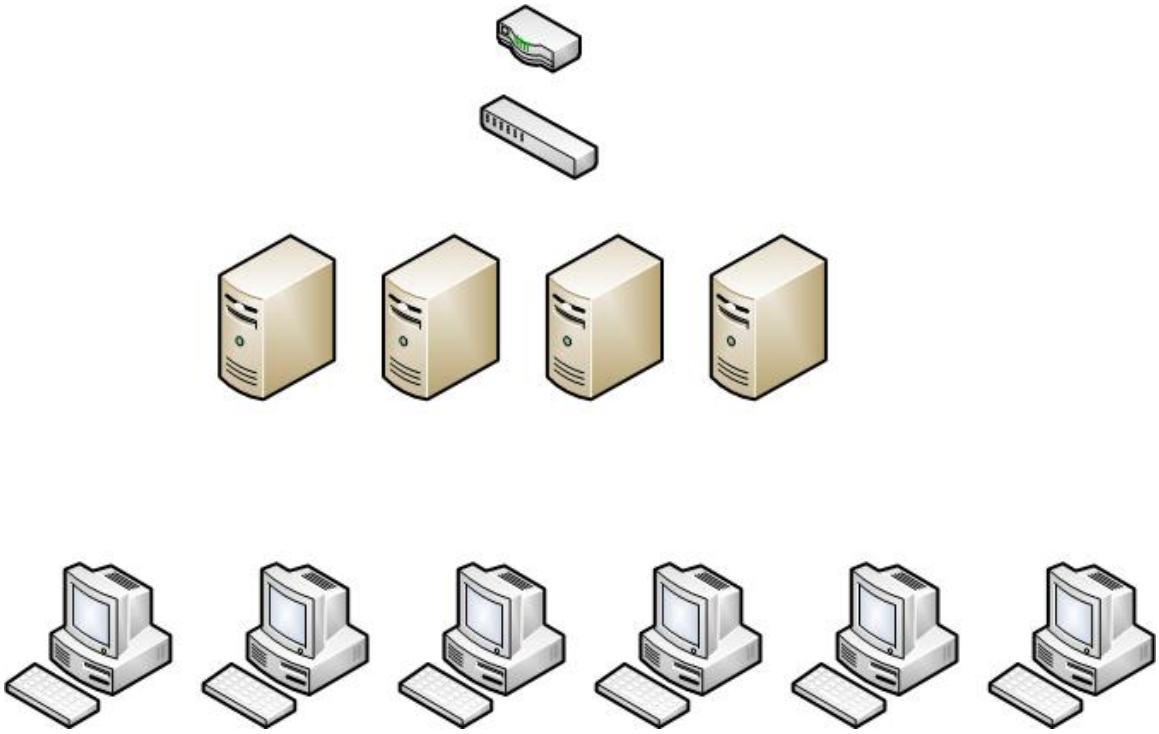
Rock Islands Consulting

Information Technology Manual

June, 2012

Table of Contents

Information Technology Network Overview



External

64.99.24.23

Internal

192.1.1.25	Router
192.1.1.1	n/a
192.1.1.2	System #1
192.1.1.3	n/a
192.1.1.4	System #2
192.1.1.5	System #3
192.1.1.8	System #4
192.1.1.101:81	Cameras

Risk Assessment, Treatment and Control

1.0 Purpose

To empower the CST to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope

Risk assessments can be conducted on any entity within RICS or any outside entity that has signed a *Third Party Agreement/Arrangements* with RICS. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs is the joint responsibility of CST and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the CST Risk Assessment Team in the development of a remediation plan.

4.0 Risk Assessment Process

For additional information, go to the Risk Assessment Process.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms **Definitions**

Entity Any business unit, department, group, or third party, internal or external to <Company Name>, responsible for maintaining <Company Name> assets.

Risk Those factors that could affect confidentiality, availability, and integrity of <Company Name>'s key information assets and systems. InfoSec is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History

Risk analysis worksheet (Range of 0.0 to 1.0 for P and I)

Threat	Probability (P)	Impact (I)	Risk = P x I
Flooding – Internal			
Flooding – External			
Fire – Internal			
Fire – External			
Severe Storms			
Wind Storm			
Earthquake			
Tornado			

Hurricane			
Snow Storm			
Ice Storm			
Hail			
Drought			
Tsunami			
Mud Slide			
Epidemic			
Pandemic			
Explosion			
Gas Leak			
Structural Failure, e.g., Bridge Collapse			
IT – System Software			
IT – Applications			
IT – Hardware			
IT – Viruses			
IT – Hacking, Unauthorized Intrusions			
IT – Communications, Connectivity			
IT – Vendor Failure			
IT – Operational (Human) Error			
Utilities – Water			
Utilities – Sewage			
Utilities – Electricity			
Utilities – Gas			
Utilities – Steam			
Utilities – Communications			
Terrorism – Biological			
Terrorism – Chemical			
Terrorism – Radiological			
Terrorism – Nuclear			
Sabotage			
Bomb Threat			
Criminal – Theft			
Criminal – Break-ins			
Criminal – Vandalism			
Criminal – Espionage			
Criminal – Hostages			
Criminal – Murder, Rape, Assault			
Criminal – Bribery			
Work Stoppage			
Work Action, Strike			
Civil Disorder			
Human Error			
Other			

Risk assessment program approved by management, communicated
Maintain and review

Security Policy

Security policy program approved by management, communicated
Maintain and review

Policy review in last 12 months

Organizational Security

Security function within the organization responsible for security initiatives

External parties have access to Scoped Systems and Data or processing facilities

Asset Management

Asset management program approved by management, communicated
Maintain and review

Information assets classified

Insurance coverage for business interruptions or general services interruption

Human Resource Security

Security roles and responsibilities of constituents defined and documented in accordance with organization's information security plan

Background screening performed prior access to Scoped Systems and Data

New hires required to sign any agreements

Security awareness training program

Disciplinary process for non-compliance with security policies

Constituent termination or status process

Physical and Environmental Security

Physical security program

Physical security and environmental controls present in the building/data center that contains Scoped Systems and Data

Visitors permitted in the facility

Communications and Operations Management

Management approved operating procedures utilized

Operational change management / change control policy or program that has been approved by management, communicated

Maintain and review

Application development performed

Third party vendor have access to Scoped System and Data

Anti-Virus / Malware program approved by management, communicated
Maintain and review

System backups of Scoped Systems and Data performed

External network connections

Wireless networking

Removable media policy approved by management, communicated
Maintain and review

Scoped Data sent / received electronically or via physical media

Web Services provided

Access and Media Liability Controls

Electronic systems used to transmit, process or store Scoped Systems and Data

Unique IDs for user access

Application development performed

Passwords required to access systems transmitting, processing or storing Scoped Systems and Data

Remote access is permitted
Information Systems Acquisition Development and Maintenance

Business information systems used to transmit, process or store Scoped Systems or Data

Application development performed

Formal Software Development Life Cycle (SDLC) process

Systems and applications patched

Web site supported, hosted or maintained that has access to Scoped Systems and Data

Vulnerability test tests (internal/external) performed on all applications at least annually

Encryption tools managed and maintained for Scoped Data

Incident Event and Communication Management

Incident Management Program

Business Continuity and Disaster Recovery

Documented policy for business continuity and disaster recovery that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy

Annual schedule of required tests – are tests done at least annually

Pandemic Plan

Business Impact Analysis conducted at least annually

Compliance

Internal audit, risk management or compliance department with responsible for identifying and tracking resolution of outstanding regulatory issues

Privacy Controls

Dedicated person (or group) responsible for privacy compliance – explain

Formally documented privacy policy (policies) – explain

Regular Privacy Risk Assessments – frequency and scope

Formal privacy awareness training for employees, contractors, volunteers (and other parties, as appropriate) – frequency and scope

Personal information about individuals transmitted to or received from non-US countries – identify countries

Process for responding to privacy incident – explain

Personal information collected directly from individuals as a service to the client – explain

Document retention program that isolates subsets of sensitive or confidential information for special handling – explain

Service provider hosts and/or maintains (as a service to the client) data about an individual, does the organization provide appropriate controls to ensure the privacy of that data - explain

Personal information – provided by the client – shared with other third parties within the US only

Personal information – provided by the client – shared with other third parties outside in the US – countries

Appropriate contractual controls to ensure that personal information shared with other third parties is protected by the third party – explain

Information security program address the protection of person information separately from other information (such as proprietary business information) – explain

Information security function regularly communicate and collaborate with the privacy function (if functions are separate) – explain

Process of ensuring the accuracy and currency of personal information at the direction of the client – explain

Process to ensure that all personal information provided by an individual is limited for the purposes described in the organization's privacy notice – explain

Third-party service providers regularly monitored for privacy compliance – explain

Appropriate sanctions applied to employees, contractors, volunteers (and other parties, as appropriate) who violate privacy policies – explain

Process for employees, contractors, volunteers (and other parties, as appropriate) to notify privacy compliance personnel of an actual or suspected privacy breach - explain