GLOBAL VULNERABILITY MANAGEMENT POLICY

10-31-2016

1. Policy

All computers, servers, applications and/or devices on Crawford's external network must be fully scanned at least monthly, for vulnerabilities. Crawford's internal network must be fully scanned on a quarterly basis. Any detected vulnerabilities must be remediated in accordance with the specific timeframes described in this Policy. To ensure that scans are comprehensive and accurate, scans should be performed by a member from ICT Security.

2. Scope

This policy governs all computers, networks, servers, applications, and/or devices automatically scanned or manually assessed by the ICT Security group.

Appendix A: Payment Card Industry (PCI) Compliance Guidelines only apply to PCI environment system components, including but not limited to computer hardware and devices, applications, network, and Internet connections. Additionally, this includes system components managed by third parties. Departures from these guidelines will be permitted only if approved in advance and in writing by the Information Security Exceptions Committee.

This policy applies to all Crawford U.S. entities, excluding Garden City Group. Violations of this policy may be grounds for disciplinary action, including termination.

3. Remediation

3.1 Vulnerability Management Remediation

3.1.1 A remediation plan must be developed for all identified high and medium risk vulnerabilities. It is expected that not all vulnerabilities will be resolved immediately (e.g., design issue within a legacy system or cost to fix it out weighs the risk or benefit).

3.1.2 Identified vulnerabilities must be remediated according to the following timeline:

Risk Level	CVSS Score	Acceptable Remediation Time
Attention	0	Discretionary
Low	1.0-3.9	Next Patch Cycle (3-6 months)
Medium	4.0-6.9	4 Weeks Max
High	7.0-10	1 Week

3.2.5 ICT Security must monitor and track vulnerabilities and progress of remediation plans.

3.2.6 Change Management policy must be followed when remediating vulnerabilities.

4. Exceptions

4.1 Review of Vulnerability Scans by Global Vulnerability Management Committee

The Global Vulnerability Management Committee will review new vulnerability scans and vulnerability exceptions as they become available during the Global Vulnerability Management Committee meeting.

5. Related Documents

5.1 Related Documents

5.1.1 Vulnerability Management Standard

Policy Name	Vulnerability Management Policy
Policy Number	Global IS Policy 00003
Effective Date	10-31-2016
Approved By	Gretchen Hiley, Chief Technology Risk Officer
Last Approval Date	10-31-2016

Exceptions to this policy must be reviewed and approved by the applicable regional Security Exceptions process.

Appendix A: PCI Compliance Guidelines

Crawford has designated a third party to manage its patches, scanning and penetration testing for the PCI environment, where this exists. ICT Security will provide oversight to ensure that these guidelines are managed appropriately.

1.1 Patching

All systems and applications must have the latest approved security patches installed. New servers and desktops must be fully patched and in compliance with the relevant configuration standards before entering production.

At a minimum, all relevant systems and applications that handle confidential or restricted information will be reviewed by the third party at least quarterly to verify compliance with the current software version and patch levels, by performing a vulnerability assessment or via manual review. The third party IT Department will monitor the release and availability of version changes and critical patches. Systems and applications should be in line with current vendor supported versions.

Any version change or patch update must first be assessed for applicability and potential risk. The third party will assess the effect of a patch on the IT environment prior to its deployment. The related development and/or deployment process is subject to Change Management Procedures. Software updates and patches must be researched, tested, and verified by appropriate personnel before installing on any system component. Prior to the application of major system updates, appropriate back-out measures must be formally documented and approved.

Any version change or patch update will be performed within appropriate timeframes, established via vulnerability assessments. System components that process, store, or transmit confidential or restricted information, must be patched within 30 days of patch availability. When system or application patches are unavailable or unable to address risks identified during vulnerability assessments, appropriate compensating controls will be evaluated and implemented.

The third party's IT Department will identify any problem with a patch and will resolve this incompatibility with the software vendor or developer of the application. If the incompatibility cannot be resolved, the third party IT Department will determine an alternate course of action, including a potential exception to this policy. Any exception to this policy must be explicitly approved by Information Security Exceptions Committee.

1.2 Vulnerability Advisories

A member from ICT Security has been designated to monitor and review all significant information security vulnerability advisories, including software patches and fixes, issued by trusted organizations to determine whether these advisories could affect any computer

systems or networks. If an advisory is deemed critical and affects critical systems or networks, System Administrators must be promptly notified and provided instructions reflecting the actions that must be taken. Non-critical advisories that could affect these same systems and networks should be batched and periodically distributed to System Administrators.

1.3 Vulnerability Rating Risk

The Common Vulnerability Scoring System (CVSS), an industry standard for assessing the severity of computer system security vulnerabilities, is used for rating and assessing the severity of system vulnerabilities. The following table represents how vulnerabilities are categorized according to the CVSS score and how remediation is prioritized:

Risk Level	CVSS Score	Acceptable Remediation Time
Attention	0	Discretionary
Low	1.0-3.9	Next Patch Cycle (3-6 months)
Medium	4.0-6.9	4 Weeks Max
High	7.0-10	2 Weeks

The risk level will be presented in the vulnerability scan report. If a score is not indicated, Medium risk level should be assumed. Immediate corrective action must be taken for the following:

- External vulnerabilities with a CVSS Score of 4 or greater; or
- Internal vulnerabilities a CVSS Score of 7 or greater.

Any systems found to have a vulnerability which has not been corrected in the acceptable remediation time must be removed from service until an acceptable corrective action has been taken. Vulnerability remediation must follow the established Change Management Procedures.

1.4 Vulnerability Scanning

Internal network vulnerability scans shall occur at least quarterly and after any significant change in the network, new system component installation, changes in network topology, firewall rule modifications, and product upgrades.

External network vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC), must occur at least quarterly.

All vulnerabilities identified should be mitigated in a timely manner to reduce risk in the environment. Documented evidence that the process has been conducted must be retained for auditing purposes.

1.5 Penetration Testing

Internal and external penetration testing shall occur at least once a year and after any significant infrastructure or application upgrade or modification. Examples of significant changes include but are not limited to, an operating system upgrade, a sub-network added to the environment, or a web server added to the environment. Testing must include both network layer and application layer penetration tests. Corrective action must be taken for vulnerabilities and exploits discovered during testing. Documented evidence that the process has been conducted must be retained for auditing purposes.

1.6 Wireless Scanning

The testing for the presence of unauthorized wireless access points shall occur on a quarterly basis, through the use of a wireless analyzer or a wireless IDS/IPS. Any unauthorized wireless technology discovered during testing should be handled according to the appropriate incident response procedures. Documented evidence that the process has been conducted must be retained for auditing purposes.