Authority	Local Government Act 1995 Local Government (Financial Management) Regulations 1996, 11

Administration 10 - NETWORKS SECURITY MANAGEMENT

Overview

Regular system updates and patching provides a mechanism for the Shire of Christmas Island to manage and protect hardware and software from security and functional issues. System updates can take the form of firmware, software, or physical hardware updates relevant to any vulnerabilities in a particular piece of hardware, software or system appliance.

The Shire considers the updates from the software service provider's security teams to be the most effective and reliable means of ensuring that that the Shire's systems are kept safe from vulnerability.

This policy defines methods and procedures used to determine what updates should be applied and timing of the updates. The following areas shall be monitored and addressed when performing system updates.

1. Purpose

1.1. This policy establishes the process for protecting assets and employees from security vulnerabilities. This policy provides procedures and supports for how updates are to be performed for all hardware and software.

2. Scope

2.1 This policy applies to all Shire staff, users, and contractors that create, deploy, or support information technology for the Shire of Christmas Island.

3. Policy

3.1 The IT Section will ensure that all systems level security updates available to the platforms and operating systems that the Shire owns, leases or otherwise have operating on our network are updated when they become available.

3.2 All updates are to be logged in the IT Officer Logbook under the Software Security Updates register.

3.3 UPDATE MONITORING

3.3.1 Several types of system updates shall be monitored from hardware software perspectives: and

a) BIOS, Firmware, and other component flash memory in appliances and computers

b) Operating systems and key management utilities

c) Productivity and application software updates

d) Miscellaneous utility software updates (e.g. Flash, Adobe Reader)

3.3.2 The Shire's IT section shall use the following mechanisms to assess requirements and the necessity for Shire's hardware and software updates:

A) Review of posted security flaws and patches for each type of hardware and software updates applicable to the system. These reviews include industry alerts, vendor notifications, or security threat notifications. If automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.

B) Automatic scanning to determine available updates and patch status of the system or application.

3.3.3 The IT Officer shall ensure regarding patches and updates that they –

a) Determine appropriate patch or configuration changes for systems and applications. Updates shall be checked no less than weekly to determine whether any new updates are required.

b) Manage a regular patching and update schedule Shire-wide that ensures all appropriate hardware, appliances, and software is checked for functional and security updates.

c) Ensure that patch and configuration change management works as designed and desired without causing other disruptions. Where possible, a test environment shall be used to validate and assess patch viability in the pre-production environment.

d) Prioritize and schedule updates and patches.

e) Maintain logs of machine patching and schedules logged in the IT Officer Logbook under the Software Security Updates register.

f) Execute appropriate Shire-wide communication to advise when patching systems.

3.4 UPDATE PREPARATION

3.4.1. Shire systems personnel shall do requisite research and testing prior to applying updates. In general, the following should be well understood before approving and applying updates:

a) The addressed vulnerability

b) Previous patches or required system updates

c) Programs affected by the change

d) Problems that may result as a result of the change

e) Procedures to back out or undo the change

f) All updates rolled out on Shire's systems are logged in the IT Officer Logbook under the Software Security Updates register

g) Where possible, new patches shall be tested in a controlled test environment that mimics the production infrastructure before they are applied. This is mandatory for enterprise applications and services where outage would cause significant organizational or ratepayer impact.

h) Staff shall ensure that backups exist of applications and data prior to installing a patch or update. Each server shall have documentation that identifies the list of applications running on the device and a patch history in the IT Officer Logbook.

3.5 APPLYING UPDATES

3.5.1 System-wide updates shall be performed on a schedule approved by the IT Officer.

Updates may be performed manually, using administrative tools, or automatically using vendor or internally provided vehicles.

a) All workstations and user systems/application (as applicable) shall have current operating system and application versions. These systems shall be patched on a regular basis as established by the IT Officer.

b) Server and enterprise application updates shall be performed by the IT Officer after the update has been tested in a non-production environment if possible.

4. Audit Controls and Management

4.1 On-demand documented procedures and evidence of practice should be in place for this operational policy. This will primarily be managed through the IT Officer's Logbook records and include;

a) Historical change management documentation as it applies to patch management processes, procedures, and protocols

b) Evidence of ongoing compliance with patching procedures including any test environments, any correspondence with software vendors, and similar.

5. Remote Access

5.1 The Shire in principle will not grant remote access to any outside organization.

5.2 Where a request to the Shire is received to do so, it must be approved by the CEO and Director of IT. The IT Officer will then be tasked to grant the third party access for a sunset period as defined by the CEO. The IT Officer will also log these requests and the outcome in the IT Officer Logbook.

5.3 Staff who require access to work emails and server access on laptops, mobile phones or other smart devices may write to the IT Officer for access. The IT Officer will record these requests as 'Operational' under the AD 9 Change Management Policy which will require approval by the Director of IT.

6. Wireless Networking

6.1 All requests for a personal communication device to be connected to the wifi network must be made to the IT Officer and approved by the CEO. Each device is to be logged with the IT Officer and the date of connection, staffer and device name is to be recorded. There may only be one personal device connected per person. The IT Officer will record these requests as 'Operational' under the AD 9 Change Management Policy which will require approval by the Director of IT.

6.2 Councillors, management and staff may request for connection. Contractors and visitors will generally be granted temporary wifi network access via the IT officer desk.

6.3 All persons who request their personal communication device connected to the wifi network must sign the SOCI Internet Fair Use Agreement. Users will agree to only use wifi access for the minimum of personal use such as online banking and payment of bills.

7. Password Management

7.1 User Network Passwords

Passwords for Shire network access must be implemented according to the following guidelines:

- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=? /~';',<>|\).
- Passwords must not be easily tied back to the account owner such as:
  - Actual name
  - Birth date

7.2 System-Level Passwords

All system-level passwords must adhere to the following guidelines:

- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use.

Please refer to AD 6 – 8 ICT Business Continuity "Emergency Temporary Access' for the break-glass provisions for emergency password management.

Document Control Box

Version	Approved, Amended, Rescinded	Date	Officer	Resolution number	Key changes/ notes	Next Review date	File Ref No.
1	Approved	21/3/2023	Chris Su	15/23	n/a	2025	