



## Guideline 4.07 - ICT Servers and Applications

### 1. Application

This guideline applies to all directors, employees and Contractors of NQBP.

### 2. Guideline

#### 2.1. Overview

This guideline relates to the servers and applications for NQBP's Information Communication Technology (ICT) systems.

#### 2.2. Server Configuration

A Server configuration is developed to support the requirements of the applications and services provided by the server.

NQBP has a number of servers at different locations within the ICT infrastructure. Servers are maintained and administered in the first instance by the incumbent IT Support service provider. IT staff with administrator privileges may also maintain server configurations, as required, from time to time.

Servers will have approved patches and upgrades applied as required to meet NQBP business needs and to provide a safe and secure environment. Security or vulnerability patches or upgrades will be applied as soon as is practically possible.

Server configurations will be documented. This documentation will provide the following information:

1. Server name;
2. Server location;
3. The function or purpose of the server;
4. Hardware components of the system including the make and model of each part of the system;
5. List of software running on the server including operating system, programs, and services running on the server;
6. Configuration information about how the server is configured including:
  - Event logging settings*
  - a) A comprehensive list of services that are running
  - b) Configuration of any security lockdown tool or setting
  - c) Account settings
  - d) Configuration and settings of software running on the server
7. Types of data stored on the server;
8. The owners of the data stored on the server;
9. The sensitivity of data stored on the server;
10. Data on the server that should be backed up along with its location;
11. Users or groups with access to data stored on the server;
12. Administrators on the server with a list of rights of each administrator;
13. The authentication process and protocols used for authentication for users of data on the server;
14. The authentication process and protocols used for authentication for administrators on the server;
15. Data encryption requirements;
16. Authentication encryption requirements;

© North Qld Bulk Ports Corporation Limited ACN 136 880 218		Document Type	Guideline	Guideline Sponsor	CFO
Version Control	Only electronic copy in RM8 is controlled. To ensure any paper copy is current, please check the policy document list on ERIC.			Revision	9
				Document Number	E17/02313
				Page	Page 1 of 2
Approval	This Guideline requires subject matter expert approval.			Date Approved	01/08/2018

## Guideline 4.07 – ICT Servers and Applications

17. List of users accessing data from remote locations and type of media they access data through such as internet or private network;
18. List of administrators administrating the server from remote locations and type of media they access the server through such as internet or private network;
19. Intrusion detection and prevention method used on the server;
20. Latest patch to operating system and each service running;
21. Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access;
22. Emergency recovery disk and date of last update; and
23. Disaster recovery plan and location of backup data.

### 2.3. Software Development

Generally, NQBP will use external vendors for any software development needs. An NQBP internal resource will fulfil a Project Management roll on any software development project. The Project Manager will oversee the development and will act as the NQBP representative for the project.

### 2.4. Commercial Off-The-Shelf (COTS) Applications and Maintenance

For most business requirements, NQBP will make use of COTS applications. Where a suitable COTS solution is not available, opportunities for modified or enhanced COTS will be investigated.

NQBP will ensure annual maintenance fees for COTS applications are paid. This will assist in keeping a minimal Total Cost of Ownership (TCO) for software applications. Typically, vendors will charge additional fees for support or upgrades when annual maintenance fees have not been paid.

## 3. ICT Guideline Policy, Procedure, Standard and Legislative Framework

NQBP is a Government Owned Corporation and port authority and is required to comply with its own policies, prescribed applicable legislation and State Government policies and procedures. This procedure should be read in conjunction with:

- a. Guideline 2.02 - Intellectual Property Management;
- b. Guideline 2.03 – Privacy;
- c. Guideline 4.03 – Electronic Communication Acceptable Usage;
- d. Guideline 4.04 – ICT General;
- e. Guideline 4.05 – ICT Security;
- f. Policy 2 – Compliance;
- g. Procedure 3.09 – Bullying, Harassment and Discrimination;
- h. Standard 2.01 - Code of Conduct.

## 4. Guideline Review Date

This guideline should be reviewed by 30 June 2020.

## 5. Definitions

**Contractors:** means contractors or consultants engaged by NQBP under a personal services consultancy agreement or other similar arrangements.

**NQBP:** means North Queensland Bulk Ports Corporation Limited ACN 136 880 128.

**NQBP Employee:** means employees and Contractors of NQBP but does not include NQBP directors.

**NQBP Personnel:** means NQBP officers (for example NQBP directors) and NQBP Employees.

© North Qld Bulk Ports Corporation Limited ACN 136 880 218		Document Type	Guideline	Guideline Sponsor	CFO
Version Control	Only electronic copy in RM8 is controlled. To ensure any paper copy is current, please check the policy document list on ERIC.	Revision			9
		Document Number			E17/02313
		Page			Page 2 of 2
Approval	This Guideline requires subject matter expert approval.	Date Approved			01/08/2018