Guideline 4.05 - ICT Security

1. Application

This guideline applies to all NQBP Personnel.

2. Guideline

2.1 Overview

This guideline relates to the Information Communication Technology (ICT) infrastructure of NQBP. This guideline is designed to protect the integrity, security and availability of NQBP information and communication systems both internally and externally.

2.2 Anti-Virus

NQBP will implement an effective software solution designed to protect against computer viruses, spyware, adware and any malicious software. The software solution will be installed and maintained on all NQBP servers, desktop computers, laptops and any other applicable device. No device is to be connected to the NQBP network without the software solution installed.

Only a systems administrator will be able to install or modify the configuration of the anti-virus software.

In the event of any virus alert or suspicious activity, users should immediately disconnect from the NQBP network and contact the system administrator for further instruction. Users should abide by the following general guidelines to minimise the possible exposure to a malicious attack:

- Do not open any files or macros attached to email received from an unknown, suspicious or un-trusted source;
- Delete spam, chain letters and other junk mail without forwarding;
- Do not download files from unknown, suspicious or un-trusted sources; and
- Scan all removable data drives before use on any NQBP system.

2.3 Firewall

NQBP computer networks will be protected by firewalls that manage direct and indirect internet network traffic.

The firewalls will be implemented and maintained by the system administrator and/or a contracted service provider.

NQBP will, from time to time, conduct a risk analysis review to ensure the firewall ruleset is adequate to afford the necessary protection for NQBP systems.

2.4 Passwords

Access to the ICT systems and resources will be through an authentication of a user name and password. A new user will be provided with an initial password that must be changed when the ICT systems are first accessed.

Passwords should be sufficiently complex to eliminate the possibility of guessing the password. Passwords must not be:

- A users name or the name of any person;
- A birth date;
- Any common acronym; or
- Any number significant to the user e.g. Number plate, driver's license.

Passwords should be:

- At least eight characters in length;
- A combination of:
  - letters (upper and lower case);
  - numbers and
  - special characters like $#@!&*.

NQBP systems will, where possible, ensure that user change their password on a regular basis and password re-use is prevented.

To maintain the integrity of the password system, users must not:

- Share their password with any other person;
- Store the password in any electronic form; or
- Write down the password.

An IT systems administrator will have the ability to re-set a users password.

2.5 Access Reviews

The permissions structure of all users with access to the Dynamics Navision ERP system will be reviewed in conjunction with the Finance team every 6 months to ensure access granted is consistent with the job function. A review of access permission to the document management system (HP RM8 and SharePoint) will be conducted every 6 months by the Senior Records Officer. Any anomalies will be reported to the CIO.

2.6 Security Classifications

Records are captured within the HP RM8 document management system and as such are assigned a security level / access control depending on the classification and content of the document.

Title of Security Level	Abbreviation	Ranking
Highly Protected	HP	40
Unclassified	UN	10
In Confidence	IN	20
Protected	PT	30
Systems Maintenance	SM	5
APT Transitional – External Access	APT	2
MCF Project	MCF	3

All NQBP employees have their RM8 profiles set to the Highly Protected (HP) security level in alignment with legislative requirements for recordkeeping. Therefore, all files and information is accessible to all NQBP employees unless the information is confidential. Individual files and documents that are confidential are locked down to select NQBP employees through access controls. Access control groups (ACGs) have been established to lock down confidential files to

specific teams or organisational departments at NQBP, examples of these include HR, payroll and legal. The different access controls are outlined in the table below.

Access Control	Description of Control
View Document	Restricts who can see the electronic document.
View Metadata	Restricts who can see the Metadata (profile form, record number, etc.).
Update Document	Restricts who can update (Edit, Check Out) the electronic document.
Update Record Metadata	Restricts who can update the Profile form.
Modify Record Access	Restricts who can update the Access Controls.
Destroy Record	Restricts who can destroy the record (Please note – NQBP has been set up so that only Administrators can destroy).
Contribute Contents	Restricts who can add documents to a container.

2.7 Remote Access

Remote access may only be granted to permanent NQBP employees. Employees wishing to work remotely must submit a business case to the CIO in support of the remote access request.

NQBP may specify minimum hardware and software computer requirements for the granting of remote access. Employees granted remote access must not store any confidential NQBP information on any remote device, mobile media or system other than the ICT systems of NQBP.

Any device used for remote access must have active real-time anti-virus software enabled.

NQBP may terminate an employee's remote access at any time.

2.8 Third-Party Access

Third Party access to ICT systems and/or resources of NQBP may be granted upon submission of a request to the CIO. The submission should clearly state the business case supporting the request.

The IT Manager may require a security assessment of the Third Party systems and protocols prior to granting access. The CIO reserves the right to conduct a security assessment of the Third Party systems and protocols at any time.

If access is granted to any NQBP systems and/or resources, it will be granted to only those systems and/or resources and only for duration sufficient to satisfy the supporting business need.

Any long term access (e.g. external hardware and software support services) is to be covered by a Service Level Agreement (SLA).

2.9 Breach

A security breach is any action or event in contravention of this policy; and/or any action or event identified as a security breach by State or Federal laws or legislation.

In the event of an employee becoming aware of a known, eminent or suspected security breach, they are to advise the CIO immediately.

The IT department will, in the event of a security breach:

- Take immediate action that will block, mitigate or contain the security breach;
- Continue action, monitor and manage the security breach until it is resolved;
- Report the security breach to relevant NQBP officials;
- Report to the relevant authorities if the security breach relates to State or Federal laws or legislation; and
- Review the events of the security breach and implement processes and procedures to prevent a future similar security breach.

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 4.04 – ICT General;
d. Guideline 4.05 – ICT Security;
e. Policy 2 – Compliance;
f. Procedure 3.09 – Bullying, Harassment and Discrimination;
g. 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.