Directive- Impact Assessment on the GNWT Network

Issued By: The Office of the Chief Information Officer

1. Effective Date: TBD

2. Application

This directive applies to departments trying to connect anything to the GNWT network such as but not limited to applications, software, hardware, upgrades and other significant changes to them. All departments, boards and agencies ("department") accessing the network, and other arm's length organizations are also required to comply with this directive. The Housing Corporation's server replacement is exempt.

3. Context

Any additions or changes requiring the network must undergo testing to ensure impacts are identified and resources are acquired if necessary. Testing is a joint responsibility and a collaborative process between the developing department and TSC.

The Technology Services Centre (TSC) provides government-wide data communications connectivity through the network. This network infrastructure provides reliable and secure connections between TSC Clients, external business partners and the internet and supports the provision of GNWT services to the public. Consistent access to key government information and resources (e.g., Internet, e-mail, web-based applications, PeopleSoft Self-Serve Portal) is provided over this network.

4. Statement

4.1 Directive Objective(s)

To ensure impacts and risks to the network are known and minimized in an effective and efficient manner.

5. Requirements

Departments are responsible for creating awareness about this directive within their environment and incorporating network testing procedures by:

- Ensuring network impacts and risk to the network are known before finalizing purchases. This should also include consulting the OCIO's Electronic Information Security standards for best

practices.

- Supplying appropriate equipment and test software, if relevant.
- Accomplishing performance limit improvements by either improving the object of the test , or acquiring additional network resources which are subject to an acceptable cost justification by the department pending a negative assessment.

The TSC is responsible for assisting Departments test new applications by:

- Supplying appropriate network equipment, and supporting department application testing requirements.
- Mitigating or restricting any changes or additions from using network resources if the application has not undergone appropriate testing and is discovered to be inappropriately using network resources or negatively impacting the security of the network.
- Reporting the mitigation or restriction of requested changes and additions to the OCIO.
- Supplying a suitable platform to run departmental applications on within the network.
- Assigning staff to work with the client Department during the impact testing. The TSC can measure the impact to the network but cannot assist with how to mitigate it.
- Setting up a segment on the test bed if the client Department is unable to test the application.
- Providing validation of the performance impact.

The OCIO is responsible for:

- Enforcing and reporting on this directive.
- Reviewing any “application restricted” reports from the TSC and for rendering a decision on future required actions if the issue cannot be resolved between the department and the TSC.

6. References

6003.10.10 Acceptable Use Policy
FAM Policies 2201 to 2206 and 2210, 3300
6003.00.26 Electronic Information Security Standards
6003.00. 26 Electronic Security Information
Procurement Guidelines

6. Monitoring and Reporting

A total of mitigated and restricted applications are reported to IPC.

7. Enquiries

All enquiries regarding this directive should be directed to the Office of the CIO.

8.Approval

Directive is effective from the date approved below.

Corporate Chief Information Officer	Signature	Date
Dave Heffernan		2016 11 18

Appendix A

All changes and additions are to follow the TSC's network test procedures before the application will be permitted to operate using network services.

Process:

1. Be aware of the requirement to test changes to existing and new computer telecommunications.
2. Allow for adequate time in your production schedule for the testing of new computer telecommunications or their enhancements.
3. Enter a service call to discuss a time for testing and other requirements such as building the pilot environment,
4. Allow between 4- 8 weeks depending on the testing. Timeframes are estimated on a case by case basis.