The Northern Territory Government (NTG) is committed to securing private and/or confidential information in its possession. For this reason, the NTG has set up a secure organisation with all the necessary resources. The Chief Minister, through the Minister of Corporate and Information Services, is responsible for supporting this commitment.

As part of maintaining a secure government, an ICT Security Framework has been established. Approved policies, standards and procedures that underpin NTG ICT security and enterprise architecture have been produced and are constantly updated to cater for the Government’s dynamic business environments internally and externally.

The ICT Security Framework forms the basis of the ICT security governance framework for the NTG. It aims to consolidate and update existing arrangements that deals with ICT security governance and it outlines:

- the responsibilities for ICT security among the various involved groups;
- the scope of ICT security policies and technical standards, and processes to ensure compliance with these policies and standards;
- the grounds for various groups to conduct investigations, and the protection offered to those under investigation;
- principles for conducting audits; and
- incident and disaster management processes.

The framework also recognises that there will be individual requirements for some agencies, e.g. NT Police, Fire and Emergency Services. As a matter of principle and good governance, these individual requirements will be discussed and resolved between the identified agency and those nominated in the framework for governance.

The principles upon which the NTG has based ICT security are in-line with current recognised best practice for Governments in Australia. There are several layers of security in the enterprise architecture model to ensure that if one layer fails, the next layer will make it more difficult to lower security. The service providers who implement the security and architecture are well trained in the suite of ICT security products in operation within the NTG.

Any organisational network is not without security incidents. These incidents are dealt with through risk based assessments. There are specific responsibilities assigned to various groups within the organisation. Similarly, disasters are dealt with through defined processes and procedures.