Self-Assessment of Stages of Development in Digital Government
Principle 4: Protecting privacy and ensuring security

This overview provides a basis to identify key characteristics of countries that have achieved early, intermediate and advanced stages of development for this principle, and the practices and policies that should be considered to progress in its implementation.

CHARACTERISTICS OF EARLY STAGE DEVELOPMENT

- *Lacks national Computer Security Incident Response Teams (CSIRT) and/or data protection enforcement authority*
- *Does not have a clear risk assessment of security incidents or privacy violations nor performance indicators in terms of systems' security*

Policies and practices to be considered

☐ Establish a CSIRT and a data protection enforcement authority

☐ Develop a risk assessment framework and indicators for data protection, *i.e.* security and privacy

CHARACTERISTICS OF INTERMEDIATE STAGE DEVELOPMENT

- *Has a functioning national CSIRT with the ability to quickly respond to incidents as well as a data protection enforcement authority*
- *Has in place performance indicators and a defined risk management approach to mitigate most or all of the risks identified through the risk assessment.*
- Has some awareness raising/capacity building initiatives to increase civil servants' sensitivity around issues related to data security and privacy (e.g. risks associated with an emerging use of social media and open government data practices

Policies and practices to be considered

☐ Develop a strategy to attract, develop and retain the necessary technical skills to ensure security and data protection in government and national IT systems

☐ Develops a strategy to increase awareness of risks and risk mitigation among civil servants and the public

CHARACTERISTICS OF ADVANCED STAGE DEVELOPMENT

- *Has strong, agile and functional CSIRTs and data protection enforcement authorities*
- *Has strong technical abilities supporting security breaches prevention and response and privacy protection*
- *Has a strong ability to collect, process and analyse data to assess risks, performance and impact of incidents*

Policies and practices to be considered

☐ Develop partnerships with the private sector to collect data (e.g. through *honey nets* and other tools) on security incidents and privacy violations

☐ Work in co-operation with international organisations in the development of strong assessment and performance indicators supporting efforts for improvement

☐ Run regular campaigns to raise public awareness and sensitivity on the emerging risks for data security and privacy