GOVERNMENT OF NEPAL
MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

Security Architecture Template

<Project Name>

Date

Version 1.0

Authors

[Name],	[Name],	[Name],

Version history

		Draft		**Final**	
Description	*Version*	*Draft Date*	*Author*	*Approval Date*	*Approver*

Table of contents

<ITALICS are special instructions for completing the template. When creating a template, insert detailed instructions in italics. Before finalising a deliverable, ***DELETE all italic text****, instructions and unused material.*

- *On Title Page: Insert document name and date of submission;*
- *On Author and Version History Page:*
  - *Author Table: Insert author names and delete generic references;*
  - *Version History Table: track ongoing history of changes to this document. Approver should be highest level person, persons or committee required to validate and adopt this document;*
  - *Copyright Version: May require adjustment based on the Terms and Conditions of the Engagement Contract. Year reference may require adjustment based on current date;*
  - *Select View>>Header and Footer to adjust Headers/Footers. Select item, right click and select Update Field.*
- *On the Table of Contents Page: Right Click within the Table of Contents. Select Update Field>>Update Entire Table;*
- *This document contains generic text and formatting references to assist in development. Adjust, duplicate by adding additional sections, build on and replace this text as appropriate for your document;*
- *When using this template to create a Technique, the following applies:*
  - *Reference the Activity(ies) or Deliverable(s) the Technique applies to;*
  - *Describe parameters of use (for example, only applies to federal agencies, only applies to specific technology);*
  - *Describe the advantages of following the technique's leading practice (for example, time savings, skills required, quality).*
- *Verify PwC] owns the copyright on any text or graphics insert into this template. Insertion of Department material or logo requires the Department's written permission. If ownership or permission cannot be verified, do not use.>*

1. Introduction

<Provide an introduction to the Conceptual Infrastructure Security Architecture Design deliverable and the process utilised to gather the appropriate information to support the creation of this deliverable. Sample text and recommended content sections are provided below. Edit, add and revise as needed to fulfill the requirements of the Department.

This deliverable may be added to and/or revised through several activities during the course of the project. At the outset of the project, you may only work on certain sections for a given activity. When beginning the "To-Be" efforts within the Assess stage, the review and profiling of the future state of the IT security environment will tend to be at a high-level, consistent with what is necessary to make strategic decisions about the infrastructure security. Detailed inventory and analysis efforts typically take place during the Design, building on the initial profile developed during the Assess stage. Please consult the Engagement Manager to find out which sections of this deliverable are required for the current activity, and which ones can be postponed until a later activity.>

It will highlight the components of the architectural framework, which could be built, identifies a constraint-free conceptual design, and outlines constraints that may be encountered when building the security infrastructure. A more detailed design will be done in later phases of the project.

1.1. Approach

<Describe the approach used to complete this deliverable. Sample text and recommended content sections are provided below. Edit, add and revise as needed to fulfil the requirements of the Department.>

The following process will be used to capture the necessary information to complete this deliverable:

- Document the Conceptual Infrastructure Security Architecture Design at the *<Department Name Here>* locations supporting the *<Program Name Here>* implementation and the *<Project Name Here>* application *<in the event that the project is driven by a major application implementation initiative.>.* The focus shall be on the review and analysis of the *<Department Name Here>* current state business unit's infrastructure security, their technical resources, and from the *<Project Name Here>* team members;
- Review the defined future state infrastructure constraints and dependencies imposed within the internal and external organisation (e.g. business issues, such as budget constraints, vendor contracts, and active/planned projects; management issues, such as leverage of existing assets and internal political concerns/boundaries; physical constraints, such as proximity to vendor/carrier sites and data centre space limitations);
- Develop an understanding of the Department's short and long-term vision of the enterprise's technical infrastructure and applications within the evolving business environment.

The scope of this document is to build upon the current policy, procedural, and reference documents already in place at *<Department Name Here>* for the *<Project Name Here>* team for those areas and activities affected by this project. This Conceptual Infrastructure Security Architecture Design document is not intended to replace current documentation; instead, this document represents a summarisation and analysis of the documents already in place. This document will validate high-level design considerations, and outline constraints that may be encountered when building the *<Project Name Here>* infrastructure. A more detailed design will be done in later phases of the project

1.2. Conceptual infrastructure security review areas

<This section highlights the organisational aspects and infrastructure security architecture areas that will be the focus of this conceptual review process, depending upon the specific needs of the project team. While different methods can be used to organize the data collected, it is important to characterise the data in a way that helps highlight the overall value that the existing security infrastructure and strategies have in supporting the current and future business, and prioritising those strategies that will be carried forward in their current form, migrated, upgraded or retired.

Additionally, the baseline activities may collect and organise information about security/integrity, legal, privacy, development, vendor support, outsourcing, or other issues critical to the business and its use of security technology. Use the following subsections as a guide to organising and executing the tasks required to complete this deliverable.

Additionally, the following sections may also be used to organise and capture the information about the enterprise's conceptual infrastructure security criteria. Compile this information into the format that is most useful for the project.

- ***Infrastructure security architecture** – Refers to all aspects of the infrastructure security structure (policy, planning, technology, systems, equipment, the administration and configurations of that equipment and systems);*
- ***Security policy** – Refers to the Policy outlining daily operational procedures and practices characteristics of the enterprise-wide or device level security policies that are written to ensure end-to-end security for network, application, and facilities infrastructure components that limit organisational exposures;*
- ***Security threats** – Refers to the identification of vulnerability in policies, procedures, practices, systems and equipment used by the Department's IT/Ops and users that represent potential threats from virus/malicious attack, unauthorised user access, unauthorised use of information, or destruction/corruption of data. The areas of focus also include the tools and documentation available to support the security threat efforts;*
- ***Network security** – Refers to characteristics of network local/remote access control, authentication, firewall protection, equipment, and security administration used by the Department's IT/Ops and users;*
- ***Software application security** – Refers to characteristics of application access control, authentication, servers, storage, and security administration used by the Department's IT/Ops and users;*
- ***Facilities security** – Refers to the physical security characteristics of the buildings, computer rooms and wiring closets, along with the access systems and types of access controls used in those same facilities or sites.*

Sample text and recommended content sections are provided below. Edit, add and revise as needed to fulfil the requirements of the Department.>

The collection of data about the enterprise and its information technology (IT) infrastructure security architecture should cover as many perspectives and dimensions relative to this project as possible. Detailed information need not be compiled, but should be available if necessary to understand the assumptions embodied in the summary.

1.2.1. Security administration

<This section focuses on the security processes and the individuals that perform those processes. Focus on simplicity vs. complexity within the Department's environment, and how security administration, management, maintenance and user interfacing complies with standard service levels. It includes the policies, procedures, and processes (manual or automated) that guide work, the location where work is performed, and the information (or reports) that are used or produced. Most deliverables have a create, update and approval cycle. Please follow this cycle as required.>

This…

1.2.2. Application security

<This section focuses on the application security processes, the applications that are used and by whom, the business rules in effect, and the data that is processed. Most deliverables have a create, update and approval cycle. Please follow this cycle as required.>

This…

1.2.3. Network security

<This section focuses on network security processes, the network security strategies that are used and by whom, the business rules in effect, and the data/reports processed, and where they are used. Most deliverables have a create, update and approval cycle. Please follow this cycle as required.>

This…

1.2.4. Technology

<This section focuses on the security technology platforms, the operational environments, who uses them, where users are located, and where they are maintained. This involves the following IT infrastructure components:

- *Application Servers;*
- *Databases Servers;*
- *Internet/mail Servers;*
- *Security Applications;*
- *Firewalls & other Network Access Components or Platforms;*
- *Physical access systems (badge access, key, access).*

Most deliverables have a create, update and approval cycle. Please follow this cycle as required.>

This…

2. Conceptual security design processes

<The following sections describe activities that are performed, the key types of work products produced, and resources that can be used to support these activities.>

This…

2.1. Conceptual activities

<The following sections describe activities that are performed, the key types of work products produced, and resources that can be used to support these activities.>

2.1.1. Analysis activities

<Utilise the Current State Infrastructure Security Architecture document findings that were analysed to determine how well the existing business processes, infrastructure components, and security infrastructure work together. The designated project team member(s) will need to conduct Department reviews of the current state infrastructure security architecture findings and validate conceptual infrastructure security architecture design strategies appropriate for the project. These review activities will be used for further determining those parts that are worth building on, and those parts that should be retired. This analysis may take the form of sets of matrices and general heuristics, such as using values of low/high or useful/not useful. The focus of the analysis is to get the most pressing concerns analysed with recommendations for improvements to ensure that the Conceptual Infrastructure Security Architecture design addresses the areas needing to be improved. Not every system identified will be improved, and not every system will be improved at the
same time

The typical areas of analysis are:

- *Work (Business): Business functions, the work that is performed, the applications that support this work, and the technology in use;*
- *Application Security Assessment: User Satisfaction versus Strategic Value; Technical Quality versus Strategic value; Technical Quality versus Technical Evolution (ease to extend and change);*
- *Application to Location: Physical locations where applications or information is accessed;*
- *Application Security to Standards: Standards/Policy employed for application security functions, software, equipment, data stores, processes, transfers (network) or development activities;*
- *Summary Application Security Assessment: Overall summary of disposition of application security, such as Keep/Tune, Asset/Build upon, Replace/Discard, Renovate/Reengineer;*
- *Application to Security Level: Levels of security/integrity that the application supports, or the level of the environment in which it operates;*
- *Security Technology: (Technology in use or planned) (Firewalls, intrusion detections);*
- *Strengths and weaknesses of current infrastructure security elements; level of standardisation; technology obsolescence; quality of security infrastructure; security infrastructure services provided and service levels, cost breakdowns, etc.;*
- *Standards to Platform: Standards implemented (partial/full/proprietary) on the various platforms), include specific versions/dates if known;*
- *Platform to Security: The technology platforms, where they operate, and the classification/ trust/integrity levels at which they operate their environment (e.g., system-high security level).*

The specific analysis process may be augmented and specialised with items specific to the scope of the project. This may include those things particular to the enterprise's business and its technological environment (e.g. centralised, distributed, global-international). The analysis team should strive to keep their terminology consistent across the enterprise. A list of references of all data sources, such as configuration management reports, inventory lists, interviews, email, and other sources, should be maintained. This will help to assess any uncertainty in the accuracy of the characterisation and help others to tap these sources again if necessary.>

This...

3. Conceptual security infrastructure architecture design

<This section would typically be included as part of other activities in the Design stage, as it will document infrastructure security architecture component details that comprise the Department's production and non-production technical infrastructure environment. Based on the high-level information gathered to document the Current State Infrastructure Security Strategy, this section may be used to drill down into components/elements of the Department's infrastructure security architecture strategy. Document strategic alternatives and design considerations that support improved infrastructure security architecture within the Department's environment, and specify if appropriate the physical and logical aspects of corporate security standards. Considerations should support simplicity within the Department's environment, and how security administration, management, maintenance and user interfacing complies with standard service levels. Some areas that could be addressed are included below.>

This...

3.1. Security policy

<Document design considerations and policy enhancements recommendations that support best practices within the Department's environment relative to this project, and if applicable, to support the appropriate security maturity model. For Example, NIST, ISO, BS, NSA, IAM, CIAC, etc.>

This...

3.2. Security threats

<Document design considerations that will reasonably address identified threats or vulnerabilities.

For example, Single Points of Failure protection in the Access and Core Network, personnel single points of failure, Denial of Service attacks.>

This...

3.3. Network security

<Document network security design considerations relative to this project that support network security improvements within the Department's environment, and any known limitations based on current technology and infrastructure architecture. For example, all components should be maintainable remotely (e.g. from NOC). Each component of the solution must be independently serviceable, Authentication – Secure Sockets Layer (SSL), Local/Remote Access Control, Firewall protection, DMZ issues, Security Administration.>

This...

3.4. Software/Application security

<Document design considerations that will address software/application security improvements within the Department's environment, and any known limitations based on current technology and infrastructure architecture relative to this project.

For example, Application Access Control, Authentication, Security Administration.>

This...

3.5. Facilities security

<Document design considerations that support physical security improvements for buildings, computer rooms, access systems and the type of access controls used in the facilities relative to this project within the Department's environment, and any known limitations based on current technology and infrastructure architecture. In addition to how security administration, management, maintenance and user interfacing complies with standard service levels.>

This…

4. Conceptual infrastructure security architecture design

<In this section, please provide a listing of any assumptions the project team has used in providing the above conceptual information. This can be offered in text format, or provided in a table pulled from a spreadsheet. Some sample assumptions could include:

- *Technology refresh process has been outsourced, and contract review was not in-scope;*
- *Legacy application consolidation project is currently in progress;*
- *Currently there is no security policy in place>.*

This…

<The following section contains possible additional paragraphs you may wish to include in your document. Use any or all of these paragraphs, or if none, then delete the entire section.

Any of the information below may be provided in a list in the body of this document, as a reference to an appendix, or as a reference to another document.>

5. Additional information

5.1. Acronyms, abbreviations and definitions

<Provide an alphabetical listing of acronyms, abbreviations, terms and definitions needed to understand this document.>

5.2. Open issues and future considerations

<If there are known issues, risks or considerations: describe, give timeframe, possible resolution>

5.3. References and related documents

<List the title, version/publishing date of referenced documents, websites, or other relevant references. If copyrighted documents are referred to, the copyright information must be appropriately referenced.>

6. Appendices

<Appendices may be used to provide information published separately for convenient document maintenance, such as classified data, or for providing supplemental material. The main body of the document should contain at least one reference to each Appendix. Appendices are listed in alphabetical progression (A, B, C).>

6.1. Appendix A – Detailed supporting documentation

This…