ISMS ENTERPRISE INFORMATION SECURITY STRATEGY

[XXXXX]

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Resource** | **Date** | **Comments** |
| V0.1 |  |  | Draft version |
| V0.2 |  |  | Reviewed |
| Vo.3 |  |  | Reviewed |

**Distribution and Sign-off List**

This document has been issued to the following people for Sign-Off(S), Review(R) or Information (I)

|  |  |  |
| --- | --- | --- |
| **Name** | **Role / Department** | **Action Required** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Page Control**

|  |  |  |
| --- | --- | --- |
| **No.** | **Item** | **Details** |
| 1. | Reference Number |  |
| 2. | Document Status | New |
| 3. | Document Classification | Internal Use |
| 4. | Effective Date |  |
| 5. | Next Review |  |
| 6. | Document Owner Name |  |
| 7. | Document Owner Title |  |

**Table of Contents**

Table of Contents

[1. EXECUTIVE SUMMARY 4](#_Toc169652565)

[2. INTRODUCTION – CURRENT STATE 6](#_Toc169652566)

[3. STAKEHOLDERS 10](#_Toc169652567)

[3.1 PLAN NAVIGATION 11](#_Toc169652568)

[3.2 Governance 11](#_Toc169652569)

[4. SECURITY MISSION AND UNDERLYING CORE VALUES 12](#_Toc169652570)

[4.1 PURPOSE OF SECURITY STRATEGY 13](#_Toc169652571)

[4.2 STRATEGIC BUSINESS OBJECTIVES 13](#_Toc169652572)

[4.3 STRATEGIC SECURITY OBJECTIVES 14](#_Toc169652573)

[4.4 MEASURING SECURITY OUTCOMES 14](#_Toc169652574)

[4.5 STRATEGIC OUTCOMES 15](#_Toc169652575)

[4.6 STRATEGIC OUTCOMES BY THEIR CATEGORIES 16](#_Toc169652576)

[4.6.1 Table 1: Improved Situational Awareness 16](#_Toc169652577)

[4.6.2 Table 2: Proactive Risk Management 16](#_Toc169652578)

[4.6.3 Table 3: Robust Crisis and Security Incident Management 17](#_Toc169652579)

[5. STRATEGIES OR INITIATIVES 17](#_Toc169652580)

[5.1 INITIATIVES 18](#_Toc169652581)

[5.1.1 Initiative #1 – Security Information and Event Management 18](#_Toc169652582)

[5.1.2 Initiative #2 – Enterprise Vulnerability and Threat Management 19](#_Toc169652583)

[5.1.3 Initiative #3 – Baseline Policies, Procedures and Standards 19](#_Toc169652584)

[5.1.4 Initiative #4 – Security Awareness for Employees 21](#_Toc169652585)

[5.1.5 Initiative #5 – Security Awareness for Executives 21](#_Toc169652586)

[5.1.6 Initiative #6 – Identity and Access Management 22](#_Toc169652587)

[5.1.7 Initiative #7 – Enterprise Business Continuity Program 22](#_Toc169652588)

[5.1.8 Initiative #8 – Enterprise Security Incident Management 23](#_Toc169652589)

[5.1.9 Initiative #9 – Certification to ISO 27001:2013 and PCIDSS 23](#_Toc169652590)

[6. SIGN-OFF SHEET FOR ENTERPRISE INFORMATION SECURITY STRATEGY POLICY 24](#_Toc169652591)

# EXECUTIVE SUMMARY

This document presents the Enterprise Security Strategic Plan for the Organization. This plan sets priorities for management, control and protection of the Organization’s information assets. The document articulates the inputs of the Information Security Community of the Organization, which comprises the Chief Information Security Office, the Head of IT, the Information Security Steering Committee (Highest Level of Executive Management) and the Information Security Working Group (Project Management).

The document highlights a 5-year vision for information security for the Organization. The 5-year vision includes 18 high-level strategic objectives grouped into the following 3 categories:

1. **Improved situational awareness**, which includes continuous system monitoring and continuous assessment of controls
2. **Proactive risk management**, with well-articulated requirements and ongoing security training
3. **Robust crisis and security incident management**, allowing critical services to continue uninterrupted in a crisis

This plan also outlines 9 key initiatives that have been prioritized for delivery during the next 2 years. These include

1. ***Security Information and Event Management*** – provide enterprise-wide security monitoring
2. ***Enterprise Vulnerability and Threat Management*** – providing ongoing vulnerability assessments of all information technology assets.
3. ***Baseline Policies, Procedures and Standards*** – complete enterprise security policy and standard framework
4. ***Security Awareness for Employees*** – ongoing and comprehensive security awareness program for all state employees
5. ***Security Awareness for Executive Leaders*** – annual security awareness event for executive management and policy makers
6. ***Identity and Access Management*** – centralized and streamlined access control solution for state government
7. ***Enterprise Business Continuity Program*** – ongoing continuity program to address unanticipated disruptions to government services
8. ***Enterprise Security Incident Management*** – enterprise-wide approach to record, identify and manage information security incidents.
9. ***Certification to ISO 27001:2013*** – enterprise-wide approach to robust information security management and management of cardholder data

Strong executive management commitment and support are essential to the implementation of this plan. Therefore, as CHAMPIONS at the highest levels, Executive Management partnership (with necessary support from the Board of Directors of the Organization where applicable) with the Information Security Office is key in effective problem solving. Successful implementation will ensure information is both protected and available and that critical Organization services are available when needed.

# INTRODUCTION – CURRENT STATE

The Organization recognizes that information is a critical asset. How information is managed, controlled and protected has a significant impact on the delivery of Organization services and on the trust instilled in the users of those services. Information assets, including those held in trust, must be protected from unauthorized disclosure, theft, loss, destruction and alteration. Information assets must be available when needed, particularly during emergencies and times of crisis.

The Organization’s ad-hoc information technology environment is inherently difficult to secure. The Organization currently operates its own data centre with many processes that are still clearly ad-hoc. Furthermore, the Organization has not defined or enforced standards limiting the diversity of hardware and software products. Current data centre consolidation initiatives will simplify the Organization’s information technology environment, making it easier to secure. However, the data centre consolidation plans will be more meaningful if they are managed in standard best practice manner.

The rapidly expanding use of the Internet for service delivery has increased the need for connectivity between the Organization and its partners, customers and even employees. This increase in connectivity has increased the Organization’s risk posture and made it more difficult to protect information. Cybercrime has skyrocketed over the past few years, shifting from crimes of notoriety to far more serious crimes for financial gain. Attackers have become much more sophisticated in perpetrating and concealing cybercrimes, typically operating in stealth mode with a goal to avoid detection.

This document is an enterprise-wide information security strategic plan for the Organization. It sets priorities for how the enterprise shall effectively and efficiently address the management, control and protection of the Organization’s information assets. It outlines the Organization’s security community’s 5-year vision, articulated as 18 high-level strategic objectives grouped in three categories.

There are significant gaps between where the Organization’s security community is today and the five-year vision. The importance of the strategic objectives was assessed prioritizing the gaps. The results of this assessment are summarized as Key Initiatives: **a two-year strategic plan**. A set of business and tactical plans detailing the deliverables necessary to achieve the key initiatives are maintained separately.

Figure 1   
Security Strategy Alignment

Security   
Strategies

Information Tech. Strategies

Major Organizational Business Initiatives

Global Threats

As depicted in the figure above, this plan attempts to align information strategic objectives with broader Organizational technology and business strategies.

This plan incorporates core information security requirements that must be in place to accomplish major Organizational initiatives efficiently and effectively. These initiatives include data centre and network improvement and the development and maintenance of major Organizational business applications, such as ongoing business applications and centralized e-commerce initiatives.

Finally, this plan incorporates global trends such as

1. More stringent regulatory requirements pertaining to information security
2. Increasing sophistication of criminals and politically motivated attackers
3. New demands to access data and services through web applications and mobile devices (i.e., laptops, mobile phones)
4. New demands to share data across multiple Organizations
5. Intense pressure to reduce costs
6. A shift from long-term employees to a more temporary and mobile workforce
7. The expanding use of software as a service.

# STAKEHOLDERS

Figure 2   
Strategic Plan Primary Stakeholders

**Executive Leadership**

**Security Community**

**Service Users**

**Enterprise**

**Security**

**Strategic Plan**

Executive Leadership and policy makers are the primary audience of this plan. From an information security perspective, they need to know the current state, the future vision, and the task necessary to bridge the gap. Achieving the strategic objectives will not be possible without strong executive commitment. Executive Leadership and policy makers must understand and have confidence in this plan. They must become problem-solving partners by committing resources and helping to remove barriers that impede progress.

The security community itself is also a key audience of this plan. In the past, critical security duties are simply not done because of lack of coordinated business justification. By joining forces to establish a common vision, the security community can ensure that all relevant departments have appropriate information security controls, and can deploy those controls cost-effectively.

Finally, business partners and customers and end users of the Organization’s services have a vested interest in the success of this plan. End users of the Organization services need to have complete confidence that the Organization will protect their data from unauthorized disclosure. End users must be confident that critical Organization services will be available when needed, particularly during times of crisis. Developing this plan demonstrates due diligence to the customers, stakeholders and partners who rely on the Organization services.

## PLAN NAVIGATION

The plan is organized into three sections:

1. **Section 2 – Mission and Underlying Core Values** – discusses the mission of the Enterprise Security Program as defined by the security community. It also outlines the core values of a security program necessary to drive the strategic security outcomes in this document.
2. **Section 3 – Strategic Outcomes** – lists the 18 high-level objectives for the Organization, segregated into three broad categories: Improved Situational Awareness, Robust Crisis and Security Incident Management, and Proactive Risk Management
3. **Section 4 – Key Initiatives** discusses the highest-priority projects that the security community hopes to accomplish during the running 2-year timeline. Additional details concerning these projects can be seen in separate Enterprise Security Tactical Plans outlined in the Risk Management, Gap Assessments and Vulnerability Database Documents.

## Governance

The Organization’s Chief Information Security Officer will lead the effort to deliver the objectives in this plan. To be successful, the Chief Information Security Officer must align and coordinate various departmental and Organizational resources with those of the Enterprise Information Security Office, a part of the Risk or Strategy Department. Furthermore, these coordinated security efforts must be vetted by all impacted stakeholders through an agreed upon governance process.

Though the governance process is still evolving, current stakeholders that participate in the decision-making process include:

1. Chief Information Security Officer (CISO) – responsible for planning, developing and deploying the Enterprise Information Security Strategy and Program.
2. Head of IT – responsible for the overall management, direction, and security of the Organization’s information assets
3. Information Security Working Group – responsible for helping develop the enterprise-wide security strategies. They help craft the policies, standards, and systems to achieve the strategic objectives.
4. Information Security Steering Committee – responsible for making sure that security efforts align with the broader Organizational technology and business initiatives. Represents executive management at the highest level in the Organization ensuring buy-in and support for enterprise-wide projects and security efforts.

# SECURITY MISSION AND UNDERLYING CORE VALUES

The following below is the security mission of the Organization

*“The Enterprise Security Program of the Organization exists to support the efficient delivery of services to our customers and strategic partners, through a sustainable information security program.*

*The program will accomplish its mission through enterprise information security policies, standards, guidelines, and services that protect the Organization’s information assets and the security interests of the users of the Organization’s services.”*

The Organization also established the following core values as a foundation for the Enterprise Security Program. The program shall

1. Increase focus on security planning activities.
2. Ensure that important security decisions are made by Executive Management (at the Highest Level) best suited to make those decisions.
3. Be comprehensive, clearly outlining the baseline requirements that the Organization must follow.
4. Have broad-based support from stakeholders who will be expected to implement the provisions.
5. Be supported by appropriate resources, including technical tools, training and people.
6. Take advantage of the size of the Organization to leverage financial and human resources to be cost effective.
7. Include methods to ensure compliance with baseline security requirements.

## PURPOSE OF SECURITY STRATEGY

The purpose of this strategy document is to provide management with the necessary information to make informed decisions about investment in security. The strategic plan links the security function with the business direction.

This strategy document identifies key business benefits and outcomes related to security with recommended strategies for achieving those outcomes.

The strategy document will serve to help achieve business objectives by identifying and addressing security requirements in business functions and initiatives, and providing infrastructure, people and processes that meet those requirements.

This strategy is flexible to cater for other factors that may impact the achievement of other outcomes. It is subject to periodic review to allow for changes in business direction and other constraining factors.

## STRATEGIC BUSINESS OBJECTIVES

The strategic business objectives of the Organization are as follows

1. To reduce costs by efficiency gains
2. To reduce potential costs through risk reduction
3. To protect assets
4. To create opportunities for revenue growth by
   1. Enhancing or creating customer services and products
      1. By creating competitive advantage
      2. Building infrastructure to provide extended customer functions
      3. Regulatory compliance
      4. Outsourcing to achieve flexibility and cost reduction

## STRATEGIC SECURITY OBJECTIVES

The strategic security objectives are as listed below

* + - 1. To reduce security events.
      2. To provide security infrastructure that reduces development costs.
      3. To protect assets.
      4. To reduce fraud.
      5. To achieve certification to standards for revenue growth.
      6. To reduce legal penalties.
      7. To reduce third party claims.
      8. To procure consulting to reduce risks.

## MEASURING SECURITY OUTCOMES

* + 1. **Metrics**

The Organization will provide methods to demonstrate when desired security objectives have been achieved or not. Metrics shall be established to determine if security processes are effective in achieving the security objectives.

Specific quantitative and qualitative measurement values shall be established to determine the impact of strategies on security objectives.

Management processes shall include planning for an outcome, implementing processes to achieve the outcome, measuring results and using the results as a measure of effectiveness to improve on the original plan.

As requirements for security controls change rapidly in response to changes in business initiatives, legislative requirements, customer expectations and new technology, measurement of security should also distinguish between the effectiveness of existing controls, and the capability of the Organization to maintain the desired level of security assurance.

The Organization shall therefore establish measures to continually identify its capabilities using best practice Capability Maturity Models.

## STRATEGIC OUTCOMES

The high-level strategies outlined in this strategy collectively define where the Organization needs to be to appropriately manage information and cyber security risks. The Security Community of the Organization believes that it will take at least 5 years to achieve these strategic outcomes, assuming that there will be sufficient resources for people, processes and tools. Without the necessary resources, the strategic outcomes will not change; however, the timeframe to achieve the outcomes will be extended.

The strategic outcomes can be classified into three broad categories:

1. Improved Situational Awareness – outcomes in this category will help the Organization obtain a better understanding of its risk posture. They also will give the Organization the ability to measure its risk posture with rigorous performance metrics.
2. Proactive Risk Management – outcomes in this category will make employees and executive management and leadership more aware of security threats. Also, they will garner the executive support needed for the Enterprise Security Program to thrive long-term. Finally, they include various types of preventive controls
3. Robust Crisis and Security Incident Management – outcomes in this category will help the Organization manage security events more efficiently and effectively thereby minimizing damage.

## STRATEGIC OUTCOMES BY THEIR CATEGORIES

### Table 1: Improved Situational Awareness

|  |  |
| --- | --- |
| SN | Strategic Outcome Description |
| 1 | All Organization systems are continuously monitored for adverse information security events |
| 2 | Information security controls are continuously assessed for effectiveness |
| 3 | Key performance indicators are used to measure the information security program’s effectiveness |
| 4 | The Organization has a consolidated and reportable information security risk profile |

### Table 2: Proactive Risk Management

|  |  |
| --- | --- |
| SN | Strategic Outcome Description |
| 1 | Executive leadership at the highest levels understand and support the information security program |
| 2 | All state employees receive ongoing security training appropriate to their job duties |
| 3 | Information security program requirements are clearly articulated in a framework of policies, procedures, and standards |
| 4 | Established relationships between the Organization and partners or customers permit shared security solutions that span traditional local boundaries |
| 5 | Executive stakeholders participate in the design and implementation of information security solutions |
| 6 | The state attracts, develops, and retains professionals with the appropriate security skills |
| 7 | Exploitable technical vulnerabilities in state computer systems are promptly identified and remediated |
| 8 | Information security controls adapt rapidly to changing risk conditions |
| 9 | People and entities that conduct business with the Organization have appropriate and timely access to the necessary computer resources and data. |
| 10 | Organization computer resources and data are protected from being used or accessed inappropriately |
| 11 | Organization stakeholders (executives, partners, customer and employees) comply with the information security program and other externally mandated compliance requirements |
| 12 | Organization stakeholders (executives, partners, customer and employees), regardless of size, are supported by security professionals and engaged in the information security program |

### Table 3: Robust Crisis and Security Incident Management

|  |  |
| --- | --- |
| SN | Strategic Outcome Description |
| 1 | When information security incidents occur, the Organization promptly contain, remediate, and manage those incidents |
| 2 | Mission critical services will continue in the event of a crisis |

# STRATEGIES OR INITIATIVES

The Organization’s Information Security Office and the Organization identify certain security outcomes and specific projects as high priority. In general, these are areas where current security controls are lax or have not been applied consistently across the enterprise, resulting in an unacceptable level of risk.

This section outlines security projects that the security community believes are high priority. It is not a complete inventory of the work being done by the security community. Rather, it is a list of key initiatives that are planned or are currently underway to address the most pressing risks. Additional details about each key initiative can be found in the Enterprise Security Tactical Plans.

The security community has identified two standards through which the initiatives will be executed. The frameworks include the ISO 27001:2013 and the PCIDSS standards.

In line with the requirements of these 2 standards, the security community has identified formal projects to address pressing concerns. Some of these security projects are now in the implementation stages.

Also of paramount importance is the certification to these two standards.

## INITIATIVES

### Initiative #1 – Security Information and Event Management

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Improved Situational Awareness* |
| *Security Outcome* | *All Organization computer systems are continuously monitored for adverse information security events* |
| *Security Strategy* | *Security Information and Event Management*  *Description:*  *Central System to provide enterprise wide security monitoring*  *Key Benefits:*   1. *Improved ability to identify complex cyber attacks* 2. *Reduced time and cost to investigate security incidents* 3. *Consistent and robust monitoring of all agencies, including those with limited resources* |
|  | |

### Initiative #2 – Enterprise Vulnerability and Threat Management

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Proactive Risk Management* |
| *Security Outcome* | *Exploitable technical vulnerabilities in Organization computer systems are promptly identified and remediated* |
| *Security Strategy* | *Enterprise Vulnerability and Threat Management Project*  ***Description:***  *Central system to provide ongoing vulnerability assessments of all information technology assets*  ***Key Benefits:***   1. *Organization finds and remediates problems before they are exploited by hackers* 2. *Inventory created of all technology assets* 3. *Services offered to all agencies, including those with limited resources* |
|  | |

### Initiative #3 – Baseline Policies, Procedures and Standards

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Proactive Risk Management* |
| *Security Outcome* | *Security program requirements are clearly articulated in a framework of policies, procedures and standards* |
| *Security Strategy* | *Baseline Policies, Procedures and Standards*  ***Description:***  *Complete enterprise security policy and standard framework*  ***Key Benefits:***   1. *Clear security baselines for all Organizational stakeholders, customers and staff* 2. *Policy-based foundation to measure results* 3. *Consistent application of security controls across the enterprise* |
|  | |

### Initiative #4 – Security Awareness for Employees

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Proactive Risk Management* |
| *Security Outcome* | *All Organization employees receive ongoing security training that is commensurate with their job* |
| *Security Strategy* | *Employee Security Awareness Program*  ***Description:***  *Ongoing and comprehensive security awareness program for all Organization employees*  ***Key Benefits:***   1. *Better awareness of security threats capable of impacting Organization’s operations* 2. *Fewer security incidents caused by employee mistakes* 3. *Common baseline of knowledge for all employees* |
|  | |

### Initiative #5 – Security Awareness for Executives

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Proactive Risk Management* |
| *Security Outcome* | 1. *All Organization employees receive ongoing security training that is commensurate with their job* 2. *Executive leadership at the highest levels understand and support the information security program* |
| *Security Strategy* | *Employee Security Awareness for Executives*  ***Description:***  *Annual security awareness event for Executive Leadership and Policy makers*  ***Key Benefits:***   1. *Clear understanding of all enterprise security initiatives* 2. *Overview of significant information security threats* 3. *Support for the Enterprise Security Program* |
|  | |

### Initiative #6 – Identity and Access Management

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Proactive Risk Management* |
| *Security Outcome* | 1. *People and entities that conduct business with the Organization have appropriate and timely access to the necessary computer resources and data* 2. *Organization computer resources and data are protected from being used or accessed inappropriately* |
| *Security Strategy* | *Identity and Access Management Project*  ***Description:***  *Centralized and streamlined access control (including biometric controlled) solution for the Organization.*  ***Key Benefits:***   1. *Better security through uniform and repeatable access control processes* 2. *Better experience for users of Organization’s services by providing all access through a single user ID and password* 3. *Reduced costs to develop new Organizational systems by leveraging an external access control solution* |
|  | |

### Initiative #7 – Enterprise Business Continuity Program

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Robust Crisis and Security Incident Management* |
| *Security Outcome* | *Mission critical services will continue in the event of a crisis* |
| *Security Strategy* | *Enterprise Continuity Program*  ***Description:***  *Ongoing continuity program to address unanticipated disruptions to government services.*  ***Key Benefits:***   1. *Faster recovery of critical government services during a crisis* 2. *Reduced costs through leveraging shared recovery environment* 3. *Better ability to share staff during times of crisis through adoption of a common plan format and tools* |
|  | |

### Initiative #8 – Enterprise Security Incident Management

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Robust Crisis and Security Incident Management* |
| *Security Outcome* | *When information security incident occur, the Organization promptly contain, remediate, and manage those incidents* |
| *Security Strategy* | *Enterprise Security Incident Management*  ***Description:***  *Enterprise-wide approach to record, identify, and manage information security incidents*  ***Key Benefits:***   1. *Ability to limit damage through information sharing* 2. *Fewer across department infections* 3. *Reduced costs through the sharing of staff and expensive forensic investigation tools* |
|  | |

### Initiative #9 – Certification to ISO 27001:2013 and PCIDSS

|  |  |
| --- | --- |
| Strategic Initiative | |
| *Outcome Category* | *Proactive Risk Management* |
| *Security Outcome* | *Information security program requirements are clearly articulated in a framework of policies, procedures, and standards* |
| *Security Strategy* | *Certification to ISO 27001:2013 and PCIDSS*  *Description:*  *Central Management System to provide enterprise wide general information security and payment card industry standard security management,*  *Key Benefits:*   1. *Improved ability to manage information security* 2. *Improved ability to manage security processes and technology surrounding the handling of card data* 3. *Consistent and robust monitoring of all enterprise wide information systems, processing facilities* |
|  | |

# SIGN-OFF SHEET FOR ENTERPRISE INFORMATION SECURITY STRATEGY POLICY