

Project Justification

IT14 - IT Security Program

Document Name	IT Security Program
Version	1.0
Reference	IT14
Issue Date	25 th October 2016
Owner	Basile Sepsakos
Author	Christie Lim

Document Control

Change History

Version	Date Issued	Issued By	Comments
1.0	25/10/2016	Paul Le Feuvre	First Issue

Note: Printed copies of this document are uncontrolled.

Document Review

The following parties have reviewed this document prior to approval:

Reviewer Name	Role	Date
Christie Lim	Information Security and Risk Manager	18/10/2016

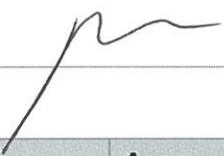
Document Approval

Approval of the Project Justification for the Security Program project is provided by the signatories shown below.

Changes to this document will be coordinated and approved by the undersigned or their designated representatives via project change management.

The undersigned acknowledge they have reviewed and approved this document.

Approver Name	Approver Title / Role
Alistair Legge	General Manager, Customer & Technology as Business Sponsor
Signature: 	Date: 27/10/16

Approver Name	Approver Title / Role
Basile Sepsakos	Head of Information Technology as Delivery Owner
Signature: 	Date: 27/10/16

Approver Name	Approver Title / Role
ISMS GG	Information Security Management System Governance Group
Approved by ISMSGG – Refer Approval Records	Date: 17/10/16

Approver Name	Approver Title / Role	
ITEF	IT Executive Forum	
Approved by ITEF – Refer Correspondence		Date: October 2016



Table of Contents

Document Control.....	2
Change History	2
Document Review.....	2
Document Approval	2
Table of Contents	4
1. Project Description	5
1.1. Objectives/Purpose.....	5
2. Strategic Alignment and Benefits	7
2.1. National Gas Rules Alignment.....	7
2.2. Multinet Gas Strategic Themes Alignment	7
3. Options.....	7
4. Economic Evaluation	8
5. Proposed Solution	9
Assumptions	15
6. Outputs.....	16
7. Project Capital Costs	17
8. Operating Cost Impact.....	18
9. Timeframes	19
10. Risks and Opportunities	19
11. Further Information.....	20

1. Project Description

The Security Program consists of a number of individual, small projects, which will allow for review, refresh, improvement and maintenance of technical and non-technical security controls to support the operational and corporate environments for both United Energy and Multinet Gas (hereafter referred to as “UE and MG”).

The costs contained in this document are for activities scheduled over the period of 2018 to 2022 and are split between UE and MG (60% UE and 40% MG) based on FTE headcount in accordance with the IT cost allocation policy.

The activities planned for 2018 to 2020 in this program are aligned with the IT Security Program submitted for the 2015 EDPR submission by United Energy.

1.1. Objectives/Purpose

The evolving security threat landscape including geopolitics, competition and innovation are making the utilities industry a prime target for nation-states, criminals and activists¹. According to the Symantec 2014 Internet Security Threat Report, targeted attack campaigns have increased by 91%, as well as, security breaches by 62% in 2013². The upward trending of targeted attack and security breaches presents a range of significant risks to the UE and MG’s operational and corporate environments, which need managing within acceptable risk parameters.

Specifically, information security incidents (reference IS002 and IS003) have been identified in the UE and MG corporate risk register as top 10 risks to the organisation. The Executive Leadership Team and the Board has recognised that information security risks, if not managed properly, may affect the sustainability and reliability of the business. A cyber security risk appetite statement was formally documented in 2016 as follow:

“We operate in an environment where cyber security threats to our business are increasing. In response to this, we seek to build and maintain a set of security capabilities that is aligned with industry standards. We aim to develop and maintain a security program and culture that focus on being vigilant and resilient towards cyber security threats – noting that our approach may vary depending upon current and emerging security threats.”

The purpose of the Security Program is to manage and maintain the operational risks related to information security by maintaining an industry baseline security environment across the logical, physical and process environments in line with the increased level and sophistication of targeted cyber security threats.

All of the activities in the Security Program are critical to success as the security protection for an organisation depends on a multiple-layer of defence model. A weak link in the overall security protection may potentially become the point of entry to the environment. [REDACTED]

¹ <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>

² http://www.symantec.com/security_response/publications/threatreport.jsp



[Redacted text block]

[Redacted text block]

2. Strategic Alignment and Benefits

2.1. National Gas Rules Alignment

The program aligns to the following National Gas Rules (NER) capital expenditure criteria:

- Rule 79 (1) the capital expenditure is such that would be incurred by a prudent service operator acting efficiently in accordance with accepted good industry practice, to achieve the lowest sustainable cost of providing services;
- Rule 79 (2) (c) (ii) the capital expenditure is necessary to maintain the integrity of services

Implementation of the projects included in this program supports the security of the network and hence its reliability and performance through prevention of security breaches that may adversely affect the network.

2.2. Multinet Gas Strategic Themes Alignment

The primary aim of the Security Program is to maintain systems to industry standards. However, it additionally supports the following strategic themes:

- Meet customer needs and growing expectations (including protecting customer privacy)
- Ensure ongoing safety, performance and resilience of the distribution network
- Ensure readiness to achieve regulatory requirements (e.g. Privacy Act)

In supporting the above themes, the Security Program helps MG achieve its business objectives of delivering customers a safe, reliable and sustainable energy supply. The Enterprise Security Architecture Framework³ demonstrates the alignment from business strategy and business attributes to security risk assessment and mitigating control selection. The Security Program CAPEX and OPEX expenditure maps back to one or more of the controls captured in the enterprise security risk assessment.

The security landscape is always changing and will continue to evolve as technology advances. By continuing to improve and enhance security a greater level of assurance can be provided to members of the public, staff, executives, the board and the regulator. Whilst the risks around information security may never be fully mitigated, MG is committed to ensure appropriate security controls are in place and commensurate with the risk to the organisation.

3. Options

The options considered for each individual project that comprise the Security Program are documented in Section 6 Proposed Solution.

³ Enterprise Security Architecture Framework v1.0 – dated November 2014



4. Economic Evaluation

The integrated nature of the Security Program and the fact that incomplete and/or partial implementation of the program has a significant impact on the evaluation of individual projects has meant that the Economic Evaluation presented here is based on “All or Nothing” and assumes the recommended solution is adopted for each project described in Section 6.

Excluding all other non-economic consequence factors related to a security incident (e.g. safety, disruption of supply, etc.), the financial impacts on MG in the event of a major security incident can be significant when taking into consideration the potential loss of productivity and potential penalty as a result of breaching contractual and/or regulatory obligations. Other intangible loss such as reputational impact and reduction in shareholder and public confidence arise because of a major security incident.

[Redacted text block]

	"Status Quo" Reference Case	Option 1: Implement IT Security Program
Net Capex (\$)	[Redacted]	[Redacted]
Opex (\$)	[Redacted]	[Redacted]
Risk (\$)	[Redacted]	[Redacted]
Least Net Cost (\$) (PV)	[Redacted]	[Redacted]
<i>Project Ranking</i>	[Redacted]	[Redacted]

[Redacted text block]

5. Proposed Solution

The Security Program consists of multiple project activities designed to support and maintain the key technology capabilities related to information security. The high-level descriptions of each element are contained within the following tables:

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
[REDACTED]	[REDACTED]



Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

⁴ http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

⁵ <http://www.cvedetails.com/vulnerabilities-by-types.php>

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Activity	Description
	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

This program was submitted to the AER (and the United Energy share of the capital funds were approved) as part of United's Energy's Electricity Distribution Pricing Review (EDPR) for the period 2016 – 2020.

Assumptions

The primary assumption is that the overall security program will be delivered as a number of projects and/or activities that progressively address known and potential security threats throughout the 2018 – 2022 period.

The program assumes that threats will evolve over the period and that whilst on-going threat assessment will refine and modify planned solutions, the impact on forecast costs will be negligible.



6. Outputs

The security program will continue to deliver the security technology capabilities required to enable the business securely. However, as the security threat and risk landscape changes over the planning period, the technology and capability will need to adapt to ensure the likelihood and impact of a security incident does not increase.

Although it is impossible to predict how changes in the security landscape will evolve over the planning period, there have been countless demonstrations since 2010 that attacks are becoming more frequent, more advanced and can be very difficult to detect and respond to.

Key technology that forms part of the security environment that are considered outputs from the security program include:

[Redacted content]

The security program will also deliver the following capabilities that will help mitigate the changing security threat and risk profile:

[Redacted content]

The option of maintaining status quo in the security front is not an option if MG wants to deliver the strategic initiatives.



8. Operating Cost Impact

The security program has an incremental impact on MG IT Operational Expenditure (OPEX). The increase in OPEX relates to increased costs associated with the following:

- Software licences, support and maintenance (application)
- Hardware support and Maintenance (including infrastructure and database related software)
- System operational support (Service desk, Incident and problem management etc)



Calendar Year	MG IT Opex \$
2019	██████
2020	██████
2021	██████
2022	██████

Notes:

- Cost reductions from retiring and/or replacing existing hardware and/or software have been taken into account in the above.
- The above table does not include other increases in opex in the 2018 to 2022 period due to the requirement for additional security services from external service providers.

9. Timeframes

The following table provides an indication of the forecast delivery timeframes for the Security program initiatives:

Initiative Title	2018	2019	2020	2021	2022	CAPEX Total
[REDACTED]	[REDACTED]		[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]				[REDACTED]		[REDACTED]
[REDACTED]		[REDACTED]				[REDACTED]
[REDACTED]				[REDACTED]		[REDACTED]
[REDACTED]		[REDACTED]			[REDACTED]	[REDACTED]
[REDACTED]				[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]					[REDACTED]
[REDACTED]		[REDACTED]			[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]			[REDACTED]	[REDACTED]
[REDACTED]				[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
				PROGRAM TOTAL		[REDACTED]

10. Risks and Opportunities

The following risks and/or opportunities have been identified in relation to this project:

- External security threats increase at a greater rate than currently envisaged such that the planned security program fails to reduce the security risk. This would leave UE & MG with a much improved security environment, but still facing a similar threat level;

[REDACTED]

[REDACTED]

[REDACTED]

11. Further Information

Industry comparisons – Compared with other Victorian Distribution Businesses, we are confident that our Security Program of activity reflects the changes required to protect the business from security related incidents.

End of Document