

**Security Primer**

A process primer for your organisation to adapt and adopt, providing assurance over security.

# Document Control

## Document Information

|  |  |
| --- | --- |
| **Date:** | 04/05/2018 |
| **Owner:** | Development Team, Eightwire, |
| **Approved by** | Jason Gleason, CEO |

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Key Deliverables** | **Author** | **History** |
| 1.0 | 2 May 2018 | Kevin Rumble | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

Document Control 2

Document Information 2

Revision History 2

*Table of Contents* 3

Table of terms used in this document 4

Background 6

Variations to this process 7

Variations should be expected 7

Variations for multiagency / multivendor systems 7

Variations for single systems 7

Variations for existing systems 7

Important information 7

Other templates and guidance to help you 8

Information classification evaluation 8

Business continuity 8

The security of health information, wherever it may exist 8

Cyber incident response and investigation 8

Guidance for offshore hosting of office productivity services 8

Privacy Act, Privacy Impact Assessment, Quick Questionnaire, and codes of practice 8

Appendix 1: Security template for signoff 9

Appendix 1: TOE Security Primer details (example template continued) 11

Appendix 2: top 4 business risks, regardless of the technology 16

Appendix 3: Top 4 technology to-do list, in preparation for installing an Eightwire agent 20

Appendix 4: top 4 technology risks, and on-going operational considerations 24

Table of terms used in this document

Terms used in this document have a specific meaning in a security context. This table provides clarity for those words where they may differ with the normalised language of your organisation.

| Description | Definition |
| --- | --- |
| TOE | Target of Evaluation (TOE). The system, site, or application that is being evaluated. In this case the Eightwire Platform. |
| DIA | Department of Internal Affairs, New Zealand, being the government-certified IaaS provider. |
| Eightwire | The platform that is used to transfer data |
| Security Certification | Security Certification is a ‘thing’. Specifically a discoverable body of evidence-based-opinion supporting assertions that as at a point in time the TOE complies with relevant minimum standards and the agreed design. Note: Certification is also a prerequisite for formal Accreditation that accepts the residual risks and authorises the TOE to operate in a production environment. |
| Security Primer | The Security Primer Package is a product of the certification process. It is compiled by the Business Owner or their delegate. The Security Primer package covers (but is not necessarily limited to):  1a) Confirm information classification evaluation, often (but not always) a national security classification assessment  1b) Business Risk Assessment / GCIO105 cloud risk assessment  1c) Privacy Impact Assessment / Quick Questionnaire (where required)  1d) Business Continuity Requirements  1e) Statement of Standards Applicable  2a) Governance and management framework  3a) Security Risk Assessment (SRA)  3b) Plans for: risk treatment, security risk management, IT service continuity  3c) Validation of design and configuration documents  3d) Security awareness program (for Data Managers that set up Eightwire projects)  3e) Planning security services for IT systems and a supporting Statement of Work, and  4a, 4b) Security Assessments (application and hosting environment). |
| Accreditation | Accreditation is the formal process to accept residual risk and then authorize a system to go into production. The Security Primer and Accreditation are commonly referred to as C&A. |
| Responsible | The role that ensures the necessary activities for a particular task gets done. |
| GCIO website | ICT.govt.nz is the official site for the New Zealand Government ICT Functional Leader, the Government Chief Information Officer. A variety of tools and templates, guidance and approaches can be downloaded from <https://www.ict.govt.nz/>that are relied on for the other processes described in this document e.g. risk assessment. |
| NZISM | New Zealand Information Security Manual <https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/> |
| PSR | Protective Security Requirements <https://www.protectivesecurity.govt.nz/> |
| DMS | Document Management System |

Background

**The primary purpose** of this document Security Primer is to assist in defining and establishing organisational security processes for on boarding Eightwire, with the aim of reducing administrative overheads for those activities.

**The secondary purpose** is to provide a basic framework for a C&A process that can be **adapted then adopted** by organisations, where no similar framework currently exists.

**This Security Primer process exists** in the <your organisation name> business process, and the Chief Information Security Officer (CISO) role <or your equivalent role> is the Certification Authority.

**The short term business objective is to** assess and evaluate Eightwire (the Target of Evaluation - TOE) for security for a particular implementation.

**The long term business objective is to** gain an understanding of Service Stewardship obligations for the validity period of the Security Primer.

**Where more than one party is responsible for a system,** the certifying authority is the lead party.

**Candidates for a Security Primer should be** subject to a formal <your organisation name> handover process into production that includes the acceptance of residual risk and authorizing its operations (sometimes called Accreditation).

**IF** the <your organisation name> business owner has sufficient budget for a Security Primer **THEN** the <your organisation name> Certification Authority may agree with the request to use this primer and/or follow this process.

**The Certification Authority in order to issue a Security Primer will need to** be convinced “…. that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met.”

**A System Security Primer does not certify that** the residual security risks are acceptable nor grant an approval to operate. That is Accreditation.

**Acceptance of residual security risks** is usually delegated to the “Accreditation Authority who will consider the recommendation of the Certification Authority, determine the acceptable level of residual; risk and issue the system accreditation, the authority to operate a system.”

The person responsible for the security policy, usually the Chief Security Officer (delegated that role by the Chief Executive) of the organisation also signs off the Security Primer to acknowledge that the intent of the <your organisation name> security policies has been meet.

**Risk assessment:** Organisations should revisit their own assessment of their business and security risks on at least an annual basis. Where there are exemptions for organisational security policies, reassess the need for each exemption.

**Recording non-compliance:** without appropriate records of decisions to risk-manage security controls, parties have less understanding of the status of cyber security within their organisation. Furthermore, a lack of such records will hinder any governance, compliance or auditing activities that may be imposed.

Variations to this process

### Variations should be expected

Variations should be expected to the Security-Primer process as described in this document. Reasons for variation may, for example, be any one or more of any of the following:

• business reasons that set milestones to align with contractual obligations and payments

• procurement process reasons, to meet the requirements of multiagency projects, and

• technical reasons, to reflect the steps used for building the product / service.

### Variations for multiagency / multivendor systems

Variations might align to the Primer milestones, defect management, and/or implementation steps. For example:

• Certify the Design

• Certify the Product(s) / Solution(s), and

• Certify each site installation for each agency

### Variations for single systems

Single system variations might deviate slightly from the traditional standard report approach shown below:

* Physical Security
* Compliance
* Change Management
* Security Policy and System Security Plan
* Risk Assessment, including Government Rules of Sourcing / Rule 13
* Operating Procedures Manual
* Decommissioning and environmental sustainability, and
* Residual risks and waivers.

### Variations for existing systems

A small variation to a large system already in certification, does not necessarily need the entire system to be reassessed. Focusing on the scope of the change, and then the steps either side (in the interests of interoperability) can reasonably contain the scope, effort and cost. For example with a data transfer variation the scope of a Security Primer might be:

* preparing the data at the source, including data hygiene checks and malicious code checks
* governance and oversight, including authorisation and obligations for annual staff training
* role based access controls (RBAC) to provide a separation of duty
* data leakage prevention (DLP) measures
* options for updates, overwrites, or new data stores in at the destination
* acceptance of incoming data at the destination: data hygiene checks and malicious code checks

|  |
| --- |
| Important information  1. All variations to the process should be approved by those in roles signing this Security Primer 2. Variations that have the potential to impact the Privacy Impact Assessment should be discussed with each organisations’ Privacy Officers |

Other templates and guidance to help you

### Information classification evaluation

Payment Card Industry Data Security Standards <https://www.pcisecuritystandards.org/document_library?category=educational_resources&document=pci_scoping_guidance>

The New Zealand Government Protective Security Requirements <https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/>

### Business continuity

Business Continuity essentials for “Value, Criticality and Sensitivity of Information” <https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf>

Further information can be found at the Business Continuity Website (Australasian Chapter) <http://www.thebci.org/index.php/home/australasian-chapter-home>

### The security of health information, wherever it may exist

Health Information Security Framework (HISFdec2015) <http://www.health.govt.nz/system/files/documents/publications/health-information-security-framework-dec2015.pdf>

### Cyber incident response and investigation

Computer Emergency Response Team New Zealand <https://www.cert.govt.nz/about/about-us/>

Reporting incidents and reporting investigations <https://protectivesecurity.govt.nz/home/protective-security-governance-requirements/reporting-incidents-and-conducting-security-investigations/>

### Guidance for offshore hosting of office productivity services

Security Requirements for Offshore Hosted Office Productivity Services Explained

<https://www.ict.govt.nz/assets/Uploads/Security-Requirements-for-OH-Office-Productivity-Jan-2017.docx>

### Privacy Act, Privacy Impact Assessment, Quick Questionnaire, and codes of practice

<https://www.privacy.org.nz/>

Appendix 1: Security template for signoff

|  |  |
| --- | --- |
| Security : Connection to Eightwire | |
| Target of Evaluation (TOE) | The <your organisation name> security zone and staging area used to send and receive information via Eightwire is what is being evaluated |
| Dates | Valid from <add date>. Valid to<add date> |
| Protective Security Requirements: InfoSec5 | As the Chief Information Security Officer (firstname lastname) I am authorised by the Chief Executive Officer to certify that assurance over security has been provided for this TOE. Specifically, that this TOE has been reviewed following a defined process. |
| The information classification of the data requiring protection | The maximum security classification of any piece of information is SENSITIVE[[1]](#footnote-1)  A Privacy Impact Assessment has been completed <add DMS link> |
| Prior certifications | Prior Security Primer’s (where they exist) for the TOE are hereby revoked once all signatories have signed this document |
| Disclaimer | This Security Primer does not mean that the TOE will be impenetrable to hackers. It does mean that all reasonable measures have been taken to: identify the information that requires protection, scrutinise security mechanisms, fix any defects, and clearly articulate and understand the residual security risks. |
| Next steps | This TOE Security Primer is one of the prerequisites for Accreditation. Accreditation authorises a TOE to operate with live data exposed to an operational environment, accepts the residual security risks, and may include a Service Stewardship programme for the validity period of the Security Certificate |
| Strength of certification | The overall security of the TOE has been tested and found to be effective for the relevant security controls selected, and the residual security risks have been identified for the Accreditation Authority to accept and be managed by a Service Stewardship programme. **It is therefore my opinion that this system can be certified.** |

|  |  |  |
| --- | --- | --- |
| Responsible  for managing the security mechanisms day to day | Accountable  that reasonable assurance over security has been achieved | Is Informed  recognises the tone-from-the-top has been implemented |
| Signature …..…..…..…………  Date ….. ….. / ….. ….. / ….. ….. | Signature …..…..…..…………  Date ….. ….. / ….. ….. / ….. ….. | Signature …..…..…..…………  Date ….. ….. / ….. ….. / ….. ….. |
| <Name>  <Role>  <organisation> | <Name>  Chief Information Security Officer  <organisation> | <Name>  <Owner, security policy>  <organisation> |

Appendix 1: TOE Security Primer details (example template continued)

| Section 1 | Start-up stage |
| --- | --- |
| 1a System security classification | Local Protective Security Requirements (or equivalent) **was/was not** taken into account when assessing this security certification  Other relevant information security classifications as per the <your organisation name> security scheme (for the information to be protected) are …   * <add DMS link> |
| 1b Business risks | A business risk assessment considers inherent risk regardless of the technology.   * A Cloud risk assessment tool, **was/was not** considered as a primer for the business risk assessment. * Reducing the likelihood of privacy breaches occurring **has/has** not included decommissioning legacy systems replaced by this TOE, as a mitigation to minimise historical technical vulnerabilities that could be exploited by an attacker. |
| 1c Privacy Impact Assessment | A Privacy Impact Assessment (PIA) for the information requiring protection was completed by <your organisations name> and is available at <add url>  Existing PIA’s for <your organisation name> can be found at <add DMS link> |
| 1d Business Continuity | <your organisation name> business critical functions that are supported by this system have already been determined, and the recovery expectations are at <add link> |
| 1e Standards applicable | The understanding of standards applicable e.g. Policy, Legalisation, Regulations Standards, to the related workflow **were/were not** agreed as being applicable by the <your organisation name> governance group for the. <add link to minutes of the meeting where discussed> |

| Section 2 | Initiation stage |
| --- | --- |
| 2a Governance and management framework | Responsibilities and accountabilities for the TOE can be found at <add link>  Regular and ongoing patch management for the TOE is provided by …. and is monitored by ….. . Key Performance Indicators (KPI’s) for patching, upgrades and malware mitigations are at <add link>  **Note:** Eightwire patching and upgrades are implemented within 2 days of publication. |

| Section 3 | Design stage |
| --- | --- |
| 3a Security risk assessment (SRA) | The Business Risk Register **was/was not** updated as a result of the SRA and the a Cloud risk assessment  The security risks for the TOE were identified and their impact understood, refer <add link>  This **did/did not** involve one or more security risk workshops. |
| 3b Risk Treatment Plan | Once the risks were identified and understood a Service Stewardship plan to was implemented, refer <add link>  Account Managers and Data Managers **have/have** not developed a basic checklist to run through before raising a cyber security event or incident <add link> |
| 3c Validation of the design | The TOE design **was/was not** noted as having implemented the recommended mitigations in the Risk Treatment Plan |
| 3d Security awareness program | The business **is/is not** ready for this change. Data Managers **are/are not** aware of their responsibilities for Eightwire projects. The Service Desk **are/are not** aware of the new software about to go into production, and technical support staff **are/are not** informed e.g. with a Known Error Database (KEDB) and ready to support the TOE. |
| 3e Planning security services for IT systems and a supporting Statement of Work (SoW) | The security services e.g. incident response capability, vulnerability assessments, penetration testing etc. (and their frequency) to be applied to the TOE **have/have not** been taken into account <add link>.  A statement of work (where required) was prepared for what needs to be tested and it also described what will be relied on <add link> |

| Section 4 | Implement stage |
| --- | --- |
| 4a Present state security assessment | Compliance reviews covered three areas:  A review of security documentation (including but not necessarily limited to):   * Existing security policies and guidance as being sufficient <add link> * Security Risk Management Plan <add link> * Incident, vulnerability and patch management <add link> * TOE standard operating procedures <add link> * a physical and technical review of the TOE and environmentals <add link> if say in an in-house server room   A vulnerability scan and penetration testing of the TOE was performed refer <add link> to detect known vulnerabilities that might allow security threats to exploit weaknesses. This testing was performed … times before satisfactory results were attained. Testing included (but was not limited to) the:   * detection of used ports available and the ability to exploit them * detection of unused software and services and the ability to exploit them * detection of weak cryptographic protocols and algorithms * the ability to exploit directory traversal   Personnel turnover was noted to **have/not have** a detrimental effect on the TOE.  Business critical functions that are supported by this system have been determined, and:   * TOE recovery expectations were specified in the business requirements <add link> * TOE Recovery Plans have been tested prior to going live and were successful <add link>   Reviews of System Recovery Plans are included in annual exercises for business continuity planning, refer <add link>  User access to the TOE is by …. over the .… network  Administrator and Superuser access to the TOE is by …. over the .… network  User access to TCP/UPD ports is minimised by …. and ….   * TOE ingress and egress gateways are described at <add link>   Time synchronization (ntp) for the TOE **does/does not** occur within a stratum (a hierarchical, semi-layered system of time sources) to add to the reliability of: workflow processing, user activity logs, audit logs, and in support of recovery activities. Refer <http://www.pool.ntp.org/zone/nz> |
| 4b Future state security assessment | Internationally-certified IaaS are used for Eightwire. Onsite physical inspection of these datacentres **was/was not** part of the evaluation process.  Modifications or additions to the <your organisation name> security mechanisms **are/are not** formally managed with change management, refer <add link>  The <your organisation name> objectives for the application of critical security patches are ….. refer <add link> |
| 4c Certification dependencies and residual risks | Mitigated risks that rely on technical mechanisms are the day-to-day responsibility of <role>, refer <add link> for a copy of the agreement.  Unmitigated risks for security are to be accepted by the Accreditation Authority and have been noted in the appendix to this Security Primer.  Dispensations (waivers or exemptions) have/have not been granted <add link>  Informational: For systems being replaced by the TOE and not reused within the organisation, decommissioning techniques for hardware should applied and the destruction certificate for any hardware should be noted.  Informational: When changing back-end cloud providers, consideration should be given to revoking previous encryption keys for the old deployment and reissuing fresh encryption keys for the new deployment. |

This document was completed for signoff on the first page by

Signature: ………………………………………………………………. ………. / ………. / ……….

Name:

Position:

Organisation:

Appendix 2: top 4 business risks, regardless of the technology

|  |
| --- |
| **Important information:** All references and annotations identified in this document are current at the time of publication. It is incumbent upon the reader of this document at the time of use to ensure that the references provided are up to date and relevant. |

| Risk title | Risk description | Suggested untreated risk rating | Examples of mitigation references | Suggested treated risk rating | Comments |
| --- | --- | --- | --- | --- | --- |
| People setting up data sharing projects may not be trained to know what they should be considering | Data Managers should be trained in the processes for data transfers between systems and the releasability authorisations required before transfers can take place. | Medium | Health Information Security Framework (HISFdec2015). Section 19 Assurance over security. Management responsibility: ‘Support security awareness, training and education requirements.’  NZISM v2.7 9.1.5.C.01. 'Agencies SHOULD align the detail, content and coverage of information security awareness and training to system user responsibilities.'  NZISM v2.7 20.1.7. ‘Using a trusted source to approve transfers …..’ | Low, given good training provides useful hints and tips on what people should consider when accepting invitations to share information | Account Managers and Data Managers need to complete and refresh their online training (on at least an annual basis) so they can:   * evaluate who sent the invitation to share and if it is appropriate * assign their users to the correct role based access control (RBAC) profiles * configure data leakage/loss protection (DLP) controls * configure the processing region (jurisdiction) * configure sharing agreement references e.g. Act, Regulation, MoU, contract, etc for each data sharing projects * respond to data sharing invitations in a timely manner * that the data tagging in place is correct and continues to be correct * take advantage of new capabilities that are introduced to any data transfer mechanisms * understand the features to stop data sharing in emergency conditions (in response to privacy or security concerns) and how to restart it again |
| Poor data transfer configuration | The Data Exchange may not be appropriately configured by organisations to run in the fastest or safest manner contrary to the MoU | Medium | NZISM v2.7 20.1.5.C.01. Agencies MUST establish a policy and train staff in the processes for data transfers between systems and the authorisations required before transfers can take place. | Low, because people configuring projects or reviewing them will be more successful if they know how to use the feature set | Training policy: Organisations should implement their own policies to train their staff to understand approved data transfer methods and how to configure and monitor them correctly. |
| Right data to the wrong destination | IF a data transfer gets sent to the wrong recipient THEN this is a privacy breach | Medium | Privacy breach guidelines from the Office of the Privacy Commissioner <https://opcwebsite.cwp.govt.nz/news-and-publications/guidance-resources/privacy-breach-guidelines-2/> | Low, where both the source and the destination agree to the sharing using a non-trivial mechanism such as a sharing-PIN | The likelihood of data going to the wrong destination in the first place is lessened by having the party responding to a data sharing invitation confirming the details of the data sharing activity using a non-trivial mechanism such as a one-off sharing-PIN. |
| Too much data becomes shared, over time | Over time the data being shared can increase from what was historically agreed.  This is sometimes called ‘accretion’ | Medium | HIPC Rule 5: (1) (a) (i) safeguards against loss  HISF Dec2015: Chapter 12, If automated outbound connection functionality is included, agencies SHOULD consider the implementation of Data Loss Prevention (DLP)  NZISM v2.7, 20.1.1. Data transfers between systems are controlled and accountable.  NZISM v2.7 17.6.7.R03. Improper decommissioning and sanitisation [or the lack of it] presents opportunities for harvesting Private Keys …. | Low, once annual reviews begin to identify sharing agreements that have been superseded so that unnecessary sharing arrangements can begin to be gracefully decommissioned. | Initial and then follow-on annual reviews of data sharing arrangements should (in addition to the points that Account Managers and Data Managers need to cover) at least consider that historical data sharing interfaces (that have been replaced) for Eightwire data sharing arrangement should, if no longer needed, be decommissioned, to reduce the likelihood of a privacy breach.  What is left behind still facing the internet that needs tidying up is sometimes referred to as ‘digital exhaust’. |

Appendix 3: Top 4 technology to-do list, in preparation for installing an Eightwire agent

| Objective | Risk description | Suggested untreated risk rating | Examples of mitigation references | Suggested treated risk rating | Comments |
| --- | --- | --- | --- | --- | --- |
| The default operating system installation has been made secure | Hardened platforms with least privilege access are less likely to be compromised | High | Advice on the top 4 strategies to mitigate cyber intrusions in a Windows environment <https://www.ncsc.govt.nz/resources/>  An objective, consensus-driven security guideline for the Apple OS <https://www.cisecurity.org/benchmark/apple_os/>  Linux audit tips for server hardening <https://linux-audit.com/linux-server-hardening-most-important-steps-to-secure-systems/> | Low | Implementation of these security baselines is said to prevent over 85% of cyber intrusions {particularly for internet facing systems] <https://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf>  **Note: The Eightwire hardening has been repeatedly tested before going live and will continue to be tested on at least an annual basis.** |
| There is only authorised access to the secure data transfer zone | Known built-in local account names and guessable passwords are targets for hackers | High | * Restricting Administrative Privileges <https://www.asd.gov.au/publications/protect/restricting_admin_privileges.htm> * Password Minimum Requirements <https://www.ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/password-standard/6-password-minimum-requirements/> * XKCD on password strength <https://xkcd.com/936/> | Low | The centralised Eightwire host based firewall is independently provisioned by each IaaS provider as a standard offering for each instance of the IaaS platform virtual image.  Client agent installations present a reduced attack surface. This is because unlike traditional data transfer software, the agent does not listen or respond to incoming communications – it only calls out to the Eightwire.   * Eightwire can provide technical details on ports used for these outgoing-only connections. |
| Only authorised software updates, are applied | Delays to applying authorised critical security patching create time-windows for hackers to exploit vulnerabilities | High | * NZISM v2.7 12.4.4.C.04. Agencies SHOULD apply all critical security patches as soon as possible and preferably within two (2) days of the release of the patch or update. * Secure WSUS (with IPsec) <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus#bkmk_2.5.ConfigSSL> * How to secure your Linux system <http://www.techradar.com/news/software/operating-systems/how-to-secure-your-linux-system-915651> | Low | Organisations are recommended to allow Eightwire to automatically patch its agent software. Patching the agent environment is an automatic and prioritised task for Eightwire.   * Allowing Eightwire to automatically patch / upgrade the agents is recommended. * Manual patching (with regard to critical security patching and/or upgrades being implemented) provides a time-window for hackers to exploit vulnerable systems. Manual patching and upgrades are not recommended. |
| Audit log files are protected against compromise | Hackers try and cover their tracks by modifying or deleting audit logs | Medium | * Mitigating the use of stolen credentials to access agency information <https://www.asd.gov.au/publications/protect/Stolen_Credentials.pdf> * OWASP audit logging cheat sheet <https://www.owasp.org/index.php/Logging_Cheat_Sheet> | Low | Audit logs are centralised at Eightwire, so even deleting an agent environment will not erase any logs.   * The Eightwire connecting agents send the logs of all their activity back to the Eightwire Platform via an encrypted channel for safe keeping. This assumes that it is harder for hackers to cover their tracks by modifying or deleting the audit logs if they can’t get to them. |

Appendix 4: top 4 technology risks, and on-going operational considerations

| Risk title | Risk description | Suggested untreated risk rating | Examples of mitigation references | Suggested treated risk rating | Comments |
| --- | --- | --- | --- | --- | --- |
| Risk assessments can be out of date | In the face of globally rising cyber threats, it is vital that organisations keep abreast of technology challenges and threats and update their organisation’s risk stance and security practices accordingly | Medium | The DIA Risk assessment process[[2]](#footnote-2)  Health Information Security Framework (HISFdec2017)[[3]](#footnote-3) 1.4 Risk management, 1.4.1 Regularly undertake a (or review an existing) health information related risk assessment | Medium, because while no risk assessment can anticipate all eventualities, | The control categories are listed the PIA section 'Assessment of privacy impacts and options for mitigation.  - Security risks assessments (to identify specific controls) should be performed before a system operates with live data and should be refreshed on at least an annual basis or following a security incident (whichever comes first). |
| Someone gets infected with malware and others are worried about catching it | Business risk: Users in both source and destination organisations might be able to override or interfere with (often mistakenly) antivirus checks on data being transferred  Technical risk: Only with mandatory (i.e. cannot be turned off by the users) automated scanning for active or malicious content is the risk of a system or network being infected actually reduced. | Medium | NZISM v2.7 20.3.1. ‘The flow of data within gateways is examined and controls applied in accordance with the agency’s security policy. To prevent unauthorised or malicious content crossing security domain boundaries.’  NZISM v2.7 20.3.5.R.01. ‘Many static file type specifications allow active content to be embedded within the file, which increases the attack surface.’ | Low, because having antivirus within organisations that is specifically tuned to their own datastore capabilities significantly reduces the time to respond to new malware circulating on the Internet.  Where Eightwire only reads data from a source and writes it to a destination, it is not transferring files, the destination systems are not expected to have their risk profiles significantly raised for file container malware | **Data source** organisations should have antivirus software in place to protect outgoing data from spreading potential malicious injection codes in the data  **At the centralised Eightwire Platform**   * **antivirus** is already installed to protect Eightwire from threats in the IaaS platform * **user-defined data leakage prevention (DLP)** can be repurposedto capture malicious commands embedded in the data   **Data destination** organisations should have antivirus software in place to protect incoming data that may contain potential malicious injection codes in the data |
| Lawful interception doesn’t seem to work anymore | **The double encryption** as implementedby Eightwire will likely interfere with existing lawful interception configurations. Those data flow paths will need to be slightly modified to re-enable interception. | Medium | NZISM v2.7 20.3.14.R.03. ‘Some systems allow encrypted content through external / boundary / perimeter controls to be decrypted at a later stage, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.’ | **Low**, because where interception is required this can still be provided by re-routing data between the agent and internal systems for inspection. Such interception may still be required for anti-virus (malware) and harmful content detection to be effective. | **The SIA has received confirmation from the relevant government agencies that the DX is not in scope for** obligations related to the Wassenaar Arrangement[[4]](#footnote-4) or the TICSA[[5]](#footnote-5) |
| Emergency stop  (veto / I forbid ) | **IF** an organisation suspects it is dealing with its own security event, **THEN** it may want to pause some or all data transfer interfaces while it figures out what’s going on and how to respond. | Medium |  | **Low,** because not only can an organisations IT support pause a connecting agent at the Windows service level, but also representatives of an organisation can individually pause data sharing projects | Data Managers need to complete and refresh their Eightwire online training (on at least an annual basis) so they can:   * start, cancel and restart data sharing as a containment measure in response to privacy or security concerns |

1. SENSITIVE includes 'For instance, where compromise could .... endanger the safety of any person'. Retrieved December 2017 from https://www.protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/#policy-and-privacy-information-security-classifications [↑](#footnote-ref-1)
2. <https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf> [↑](#footnote-ref-2)
3. <https://www.health.govt.nz/system/files/documents/publications/health-information-security-framework-dec2015.pdf> [↑](#footnote-ref-3)
4. <https://www.mfat.govt.nz/en/trade/trading-weapons-and-controlled-chemicals/which-goods-are-controlled/> [↑](#footnote-ref-4)
5. <https://www.ncsc.govt.nz/ticsa/> [↑](#footnote-ref-5)