SOCIAL WELLBEING AGENCY | TOI HAU TĀNGATA

Security Assessment

Data Exchange (DX) Platform 2022 Re-Certification

Report Data

Name of Initiative

Data Exchange (DX) Platform Re-Certification

Business Owner

Dorothy Adams, CE Social Wellbeing Agency

Stakeholder(s)

- Social Wellbeing Agency (SWA) (the lead agency and CISO)
- Eightwire Limited (the service provider)
- Agencies and NGOs (subscribers to the service)
- Revera (infrastructure provider for New Zealand based processing servers)
- Amazon Web Services (AWS) (infrastructure provider)

Objective ID

TBC

Reference Documents

- Data Exchange Control Assessment Report
  TBC
- SIA DX C&A boundary
  https://objective.ssi.govt.nz/documents/A12785930/details

Document History

Author / Reviewer	Date	Version	Description
Daniel Atkinson	25 August 2022	0.1x	Initial Drafts
Daniel Atkinson	11 November 2022	1.0	Release
Daniel Atkinson	18 November 2022	1.1	Updated SC06
Daniel Atkinson	25 November 2022	1.2	Updated C21

Overview

Description of Initiative

The Social Wellbeing Agency (SWA) supports social sector organisations to improve their data sharing maturity. As part of this work, SWA encourage and facilitate the uptake of the Data Exchange (DX), a commercially available product owned and operated by a Wellington New Zealand based company named Eightwire. The cloud platform helps to facilitate data sharing practices across the sector that are safe, secure and controlled. The Data Exchange:

- Provides a safe, secure and controlled cloud-based exchange platform.
- Connects organisations in a way that's easy, consistent and efficient.
- Promotes standardised approaches to privacy, data management and data standards.

The DX was certified in November 2020 for information classified up to SENSITIVE, for a period of 3 years. However, the service provider is rearchitecting how the solution is delivered and is moving components of the solution from Microsoft Azure to Amazon Web Services (AWS). Therefore, a recertification of the platform is required.

This current initiative is the re-certification of the DX for 3 years.

Nature of Information being handled

The information processed and transferred by subscribers of the DX is not stored within the DX. Once the information has been processed and transferred it is removed.

The following information is stored within the DX:

- Metadata that defines the data types transferred by the DX.
- Subscriber information.
- DX user, administrator, and system credentials.
- System configuration.
- System logging information.

The DX is used by various agencies and as such the information processed and transferred by the DX is varied. In previous risk workshops (held in 2020) with two subscribers of the DX (Accident Compensation Corporation (ACC) and the Department of Corrections) the following information types were determined as being processed by the DX:

- Personal information, including but not limited to names, dates of birth and addresses.
- Medical information.
- Service provider contract reporting data.
- Anonymised and summarised data.

The compromise of information processed and transferred by the DX is likely to damage New Zealand's interests or endanger the safety of its citizens. (https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/policy-and-privacy-information/).

It is not the intent or the purpose of the DX to handle national security information (RESTRICTED and above).

Information Classification:	SENSITIVE
Impact if Confidentiality breached:	For a subscribing agency, the consequence would be **Severe** if the **confidentiality** of information is compromised due to the sustained media coverage and resulting reputational damage. There would be a significant impact on the ability of the agency to deliver services via the Data Exchange. The public would lose confidence and trust in the subscribing agency. As the lead agency, the consequence to SWA would be **Severe** if the **confidentiality** of subscribing agency information is compromised, if it is found that there are systemic weaknesses within the DX and multiple agencies are impacted.
Impact if Integrity breached:	For a subscribing agency, the consequence would be **Moderate** if the **integrity** of information is compromised, as there would be a disruption to service delivery with a moderate impact on customers and/or key stakeholders. If incorrect data were relied upon by an agency, there would be some reputational damage to the agency. As the lead agency, the consequence to SWA would be **Moderate** if the **integrity** of subscribing agency information is compromised. If incorrect data were relied upon by a subscribing agency, there would be some reputational damage to SWA as stakeholders may lose confidence in the service.
Impact if Availability breached:	For a subscribing agency, the consequence would be **Moderate** if **availability** of the DX is compromised for a period of up to 1 day. There would be disruption to service delivery with moderate impact on customers and/or key stakeholders As the lead agency, the consequence to SWA would be **Minor** if **availability** is breached for a period of up to 1 day, as there would be a minor impact on SWA objectives and strategic outcomes. Repeated or extended outages of the platform may lead to an increase of the consequence level.

Summary of business process / information flows

The DX supports a multitude of business processes depending on the individual requirements of each subscriber.

The DX allows agencies to install software agents on their systems or to use a browser-based drag and drop application to share information with other subscribers of the DX.

When using the agent, a subscriber to the DX will install and configure the software agent to share selected information via the DX. The agent supports information stored in various sources, including databases and files such as excel spreadsheets. The DX can take information stored in one format and transform it into another format before delivering it to a subscriber. The agent does not accept inbound network communications. The agent establishes an outbound connection from a subscriber's system, where the agent is installed, to the DX. The DX does not retain the information that is transferred.

Cloud data sources are also supported by the DX and do not require a software agent to be installed. Cloud data sources connect directly to the DX.

The DX provides direct API access. This allows agencies to programmatically interact with the DX to streamline workflow.

Subscribers to the DX access a web portal to configure the service. The web portal is used to:

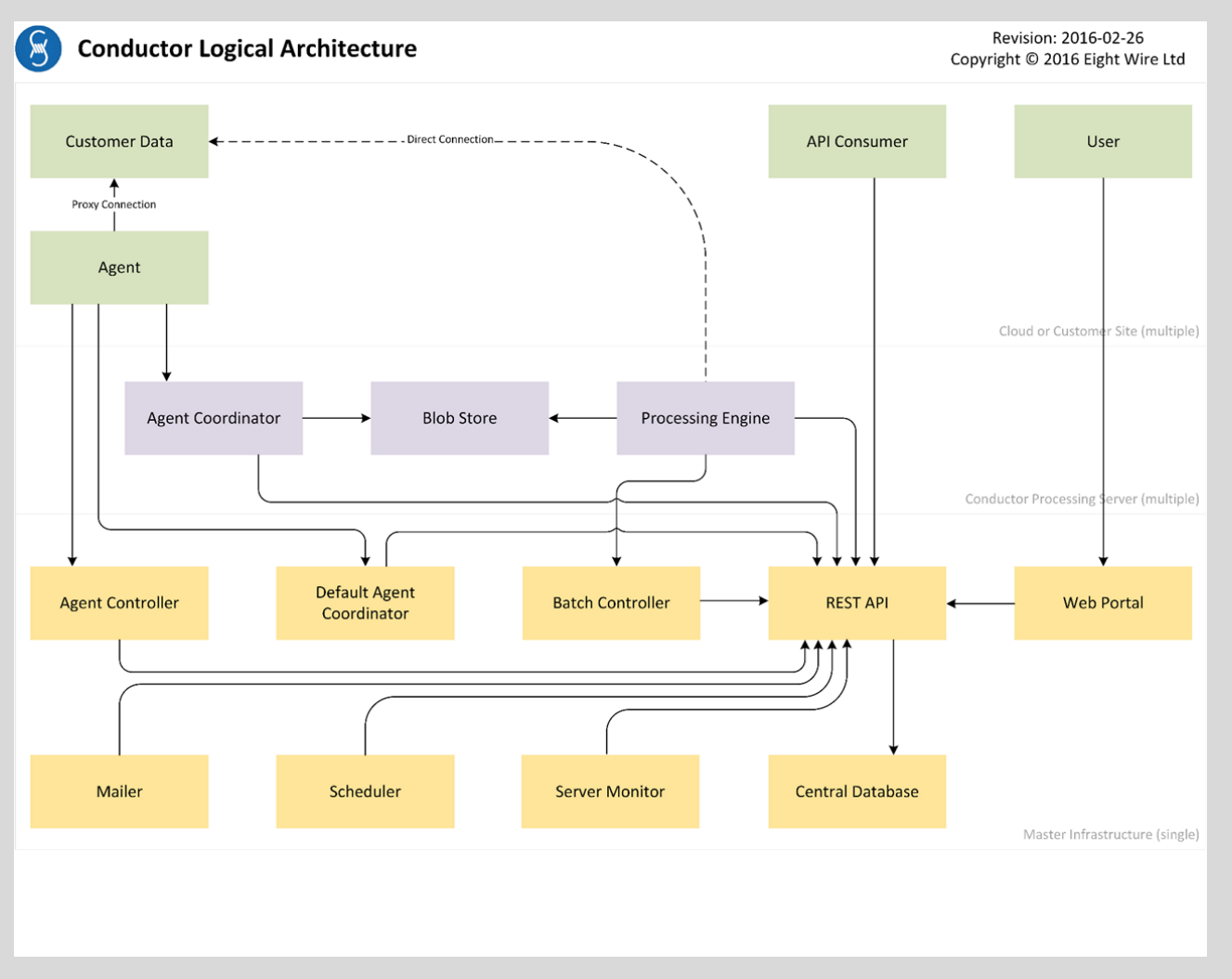
- Create and manage subscriber administrators and users.
- Configure agents.
- Configure information sharing with other subscribers (allowing subscribers to reference a sharing agreement)

Software agents interact with an agent controller. The agent controller manages all agents. It receives 'heartbeats' from the agents and if there is any work for an agent, responds to the agent's heartbeat with a set of commands for the agent to follow. The agent controller waits for agents to make contact – it does not initiate contact with any agents.

A default agent coordinator is used to handle agent software updates and to gather performance information about all agents.

Processing servers are where the information is sent for processing by the DX. Multiple processing servers exist to ensure availability, including within New Zealand for agencies that have onshore requirements. The batch controller is used to manage all processing servers.

All metadata and service configuration data are stored in the central database.



Description of systems

The DX is based on Windows technology and is predominantly hosted on managed containers within AWS, in Australia. Processing servers (Windows servers) are also located in Revera Datacentres in New Zealand to support subscribers that have onshore processing requirements.

The central database, used to store metadata and service configuration data, is an AWS managed serverless Microsoft SQL instance.

Geographic location of information:	Australia and New Zealand (New Zealand based processing servers can be selected by agencies, if required).
Nature of cloud service model:	Software as a Service
Independent Certifications:	Independent certifications of the vendor, and existing government and third-party certifications

	for AWS and Revera will be leveraged where possible.
Publicly Accessible:	Yes (For authenticated users)

Scope

Security - Full Scope

The scope of the initiative is to complete a full re-certification of the DX. This includes:

- Reassessing the risks identified during the previous certification, based on the current threat landscape.
- Reviewing the security controls selected to manage the identified risks.

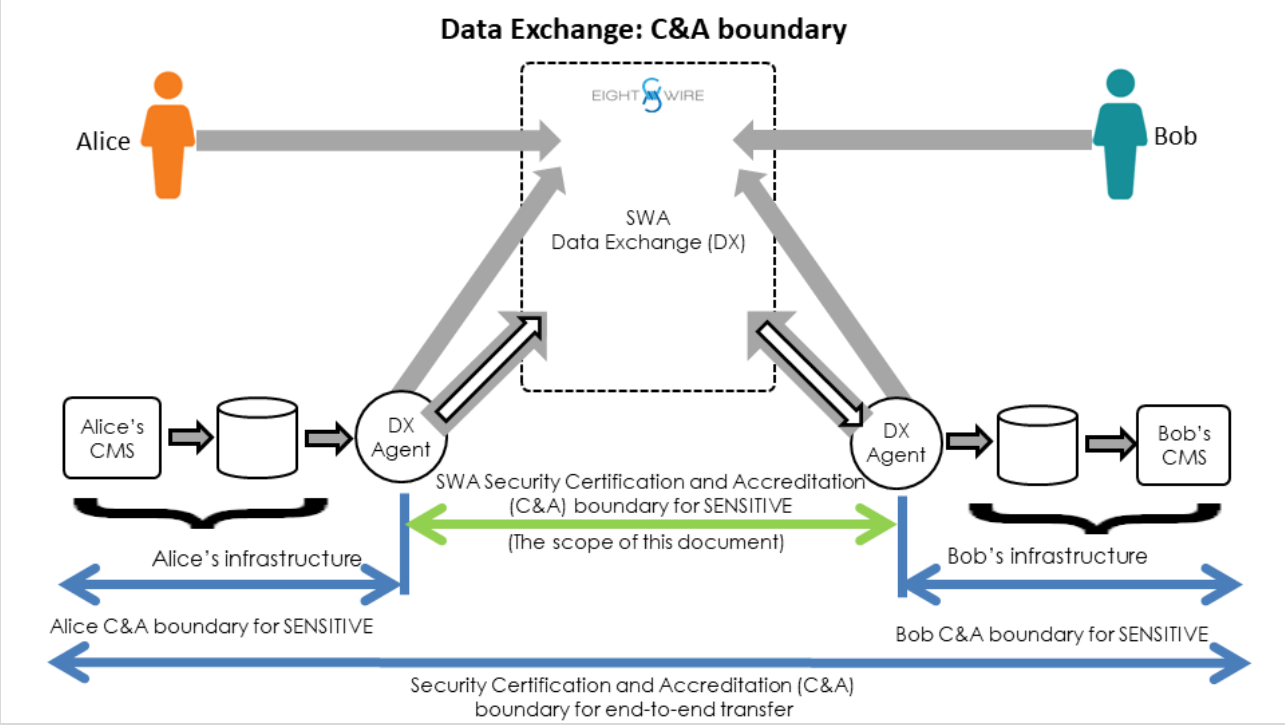
The following components are in scope:

- The software agent that is installed by agencies. The agent is used to send and receive information to and from the DX.
- The DX web application and all associated components (shown in yellow and purple in the logical diagram above).
- The AWS container platform on which the web application and all associated components are hosted.
- The Eightwire configurable elements within the AWS and Revera platforms.

The following components are **out** of scope:

- The underlying AWS IaaS infrastructure.
- The underlying Revera IaaS infrastructure.
- Agency systems, including systems:
    - where the agent is installed.
    - used to logon to the portal.
    - that interface with the DX API.
    - that provide network services to a subscriber.
    - configured as a data source.

The scope is shown in the following diagram and is represented by the middle arrow:



A subscribing agency's servers, data sources and infrastructure are outside the scope of this certification. The above diagram shows that for an end-to-end transfer there are components outside the scope of this platform re-certification. This risk assessment provides an agency with guidance on the security controls that they are responsible for configuring within the Data Exchange, and within their environment. It is a subscribing agency's responsibility to ensure the implementation and ongoing management of these controls, and to seek assurance from other parties with whom they share information.

It is a subscribing agency's responsibility to review this risk assessment and certification within the context of their intended use of the platform, and to identify any additional risks that may apply.

The current residual risk level identified in this security risk assessment assumes a subscribing agency has implemented and is maintaining the security controls identified as an agency's responsibility.

The certification and accreditation of the DX by the lead agency (SWA) does not remove the requirement for a subscribing agency to complete their own assurance activities. There are configurable elements in the DX and security controls within a subscribing agency's environment that a subscribing agency is responsible for implementing and maintaining. As the lead agency SWA works with the vendor to ensure the platform is maintained and operated securely, and to provide guidance to subscribing agencies on how to configure and use the DX.

When the sending and receiving subscribing agency have certified the platform for their use, the end-to-end transfer is certified for SENSITIVE.

Summary of Findings

Security

During the control validation Eightwire were proactive in resolving issues that were introduced with the move to AWS.

Controls that are assessed as partially effective or not effective do not prevent the solution from meeting the target risk level. Recommendations to implement these controls are provided to ensure defence in depth.

The new AWS environment is built and deployed using infrastructure as code (IaC). This ensures consistency of deployments across production and pre-production environments. IaC provides assurance that controls are properly configured when environments are deployed or refreshed, and allows control configurations to be reset to, and evaluated against, a known good state.

It must be noted that all control validation was performed prior to customers being migrated to the new platform. This was done to ensure that all controls were implemented prior to cut over.

A web application penetration test was not conducted with the re-platform to AWS. A web application penetration test was completed against the DX in July 2022. To provide assurance, ZX Security independently reviewed the changes to application code and configuration that have been made for the DX to be hosted in the AWS environment, to ensure that no weaknesses have been introduced.

When selecting controls to manage the identified risks, the controls have been split between a subscribing agency, the lead agency, and Eightwire as the service provider. The provides each party with a clear indication of who is responsible for the implementation and management of a control.

Risk Profile

Overall, there are 16 medium risks, 4 low risks and 6 very low risks associated with the Data Exchange. This is the current residual risk level based on the assessed effectiveness of the recommended controls. The risk matrix below summarises the risks

All identified risks meet their target residual risk level. Target residual risk is the level of residual risk anticipated after the remediation of any ineffective or partially effective

controls. Although all risks are being managed to the target risk level, a remediation plan is provided for controls that were deemed to be partially effective, or as ineffective.

The target risk levels were still achieved where controls were deemed to be ineffective or partially effective due to the implementation of compensating controls (that were initially recommended to provide defence in depth) or due to other mitigating factors. Additional information is provided below in the "Commentary on Risk Profile" section, and in the detailed risk table in Appendix 1.

The controls that manage the identified risks were assessed. Of the controls identified as key controls all but one was found to be effective within the context of the identified risk. This control (Eightwire staff screening) was assessed as partially effective.

A remediation plan has been agreed as part of the sign off in Nov 2022. The remediation plan has set a date of 28 February 2023 for all remediation to be complete.

The current residual risk level has been assessed on the assumption a subscribing agency has implemented and is maintaining the security controls identified as an agency's responsibility.

The details of the control assessment activities are included in Appendix 2.

LIKELIHOOD	CONSEQUENCE: Routine	Minor	Moderate	Major	Severe
Almost Certain					
Likely					
Possible					
Unlikely		SR07 SR13 SR17 SR21		SR02 SR05 SR06 SR11 SR26	
Rare		SR08 SR12 SR14 SR15 SR16 SR18		SR01 SR03 SR04 SR09 SR10 SR20 SR22 SR23 SR24 SR25 SR27	

KEY: Target Residual Risk: **R##** Current Residual Risk: **R##**

Target Residual Risk = Current Residual Risk: **R##**

Security Risks: SR## Privacy Risks: PR## Human Rights Risks: HR## Ethics Risks: ER##

Commentary on Risk Profile

Many of the risks identified have a current residual risk level of MEDIUM due to the inherent risk consequence level of SEVERE. There are a limited number of controls available to manage the consequence of a risk where the confidentiality of information is compromised, and it is not always possible to reduce the consequence by more than a single level.

The controls selected to manage the consequence allow Eightwire, the lead agency, and a subscribing agency to investigate, proactively manage, contain, and recover from, an information security incident.

Based on the assessment of the implemented controls the likelihood of all identified risks has been reduced to UNLIKELY or RARE. However, should a risk still eventuate the consequence to an agency would be MAJOR for the risks where the confidentiality of information is compromised.

All controls identified as ineffective and partially effective should still be implemented (or the identified weaknesses remediated) to strengthen the control environment and to provide defence in depth. The controls identified as ineffective and partially effective form the basis of the remediation plan included in this report, with priority given to the key controls.

Remediation Plan

The table below outlines the **agreed remediation activities**. The control details, including results of assessment activities are included in Appendix 2.

Control Ref & Title	Agreed Remediation Activities	Impacted Risks
C06. Screening	Ministry of Justice background checks have not been completed for all Eightwire staff. There are two contractors who are based overseas that have not had Ministry of Justice (or their local country's equivalent) background checks completed. **Remediation agreed with Responsible Manager** Once background checks have been completed for all Eightwire staff Eightwire to report to the lead agency the outcome. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023	SR09
C21 Encryption of Data in Transit	The AWS configuration review identified S3 storage buckets that do not enforce transport layer encryption on HTTP connections, however these buckets are blocked from public HTTP/S access and are only accessed by other internal resources in AWS. It is a best practice to set this HTTPS condition on bucket policies regardless, and Eightwire do have this on their security improvement backlog. **Remediation agreed with Responsible Manager** Set the HTTPS condition on bucket policies. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023	SR10 SR16
C22 Encryption of Data at Rest	Customer data is only stored in the RDS SQL databases for Conductor and Blob, and this is encrypted. There are AWS S3 storage buckets that are not encrypted. These are not used to store customer / sensitive data.	SR16

	The Agent configuration is encrypted once the agent update process has completed. In testing by ZX Security, it is not encrypted after the initial install. **Remediation agreed with Responsible Manager** Encrypt all AWS S3 storage buckets (for defences in depth). Ensure the agent configuration is encrypted during the initial install process. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023	
C50. Contractual Agreements and SLA	It is recommended that Agencies identify their security requirements and include these in any contracts with Eightwire. **Remediation agreed with Responsible Manager** Eightwire can be proactive and include many of these in the contract as standard, showing how they securely manage and maintain the platform, such as: • Logging and auditing, including retention. • Patching process and timeframes. • Platform security testing (such as penetration testing) schedule. • Configuration review schedule. • Customer right to audit. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023	SR01 SR03 SR05 SR07 SR08 SR17 SR18 SR23
SC06 Agency Data Restricted to NZ	When New Zealand processing servers are selected, the DX correctly routes transfers via the processing servers that have been deployed to simulate New Zealand based servers. However, until the cutover is complete, these "New Zealand" processing servers are temporary virtual machines located in AWS Australia.	SR15

	The New Zealand processing servers that are used in the current environment will continue to be used once the cutover is made. It is not possible to test this prior to cutover. **Evidence to be provided after go-live** Eightwire to provide evidence that New Zealand hosted processing servers are used when selected by the customer. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** Once cutover to new environment has been completed.	
SC13. Timeout Password Reset Links	Password reset links do not currently timeout. Please note this was marked as resolved in 2020, however testing shows that links do not timeout. **Remediation agreed with Responsible Manager** Eightwire to configure the password reset links to timeout after 60 minutes. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023	SR27

Approvals

Certification

☐ Certified
☐ Qualified Certification
☐ Not Certified

Comments

[If some controls cannot be assessed until system / process is live, note here the controls that require evidence and by when. Depending on the significance of these controls consider whether full or qualified certification should be given]

[comment on any enterprise controls that are not going to be in place and why not. Note that the Current Residual Risk in these areas needs to be accepted]

Chief Information Security Officer / Chief Privacy Officer Date

I confirm that this report accurately represents the security and privacy risks associated with the identified scope and that the controls relied upon in this assessment are in place and operating at the time this certification was provided.

Accreditation

☐ Accredited
☐ Qualified Accreditation
☐ Not Accredited

Comments

Business Owner name, title Date

I accept the current residual risks as outlined in this report and I confirm that the remediation plan (if any) will be implemented within the indicated timeframes.

Appendix 1 – Risk Assessment

Security Risk Assessment

The table below details the information security risks identified based on the effect they have on the confidentiality, integrity and availability of Agency data. The controls in **bold** are the key controls and have the strongest effect on reducing risk. The control detail and results of assessment of control effectiveness is outlined in Appendix 2.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
Risks SR01-SR19 are from the previous Security Risk Assessment certified in 2017. The risk levels and control requirements have been reassessed, and scenarios have been defined.							

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR01	**Web portal credentials are compromised:** Credentials for the web application are obtained by phishing or social engineering, which may result in an attacker gaining access to an Agency's Data Exchange web application account and stealing information that is shared using the Data Exchange. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A malicious person obtains valid credentials to the service through a phishing campaign. Once logged in, the malicious person downloads and installs the agent. Any file based datastores are replicated on the local device and used to receive information transferred through the DX. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C08. Security Awareness(L)** • C16. Management of Privileged Access(L) • **C17. Multi-Factor-Authentication (enable) (L)** • C19. Access Control (configure)(L) • **C54. Information Security Incident Management(C)** • SC01. Email Protection(L) **Lead Agency Responsibility** • **C26. Standard Operating Procedures (for onboarding process) (L)** • C50. Contractual Agreements and SLA (with Eightwire to define reporting requirements) (L) **Eightwire Responsibility** • **C08. Security Awareness (keep up to date with social engineering techniques) (L)** • **C17. Multi-Factor-Authentication (implement capability) (L)** • C18. Password Management System (implement capability) (L) • C19. Access Control (implement capability) (L) • C23. Cryptographic Key Management (protect web server certificate) (L) • C26. Standard Operating Procedures (for validating a customer's identity for requests to disable MFA or to reset passwords) (L) • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • C48. Secure Application Development (XSS and CSRF protection) (L) • SC01. Email Protection (SPF Records) (L) • SC08. Service Reporting (report of accounts **not** using MFA) (L)	**Medium** Major / Rare		**Medium** Major / Rare	The likelihood is reduced by: • An agency enabling multi-factor authentication within the web portal to protect against scenarios where an attacker has been able to obtain a user's credentials. • Agencies and Eightwire providing their staff with security awareness training to keep them abreast of current threats and methods used to obtain a user's credentials and providing guidance on how to securely generate and store passwords. • The lead agency providing guidance and configuration recommendations during the onboarding process to enable security controls. A checklist has been developed as part of the onboarding pack. • Eightwire providing the lead agency with regular reports of agencies that have not configured control recommendations (for this risk, multi-factor authentication). The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. *The key control to manage this risk is the use of Multi-factor authentication. As a cloud platform it is a subscriber's responsibility to enable multi-factor authentication for their account.*

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR02	**Agency data is deliberately shared with a non-authorised party:** An Agency/NGO sends their data (or makes it available) to a person or organisation outside of their accepted list. This may result in the unauthorised disclosure, loss or modification of sensitive data. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. **Example Scenario(s):** • An agency administrator sets up a data sharing process with an organisation that they are not permitted to share information with, and the receiving party does not protect the information. **Affects:** ☒ Confidentiality, ☒ Integrity, ☐ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C07. Role-Based Training (L)** • C16. Management of Privileged Access (L) • C19. Access Control (configure) (L) • **C54. Information Security Incident Management (C)** • **C62. Security Tests and Controls Audit (L)** • **SC03. Acceptable Data Assurance (configure) (L)** • SC09. Memorandum of Understanding (L) **Lead Agency Responsibility** • **C07. Role-Based Training (L)** • **C26. Standard Operating Procedures (for onboarding process) (L)** **Eightwire Responsibility** • C19. Access Control (implement capability) (L) • **C26. Standard Operating Procedures (for agency use) (L)** • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • SC03. Acceptable Data Assurance (implement capability) (L) • SC09. Memorandum of Understanding (provide the ability to record agreements within the DX) (L) • **SC11. Sharing One-time Code**	**MEDIUM** Major / Unlikely		**MEDIUM** Major / Unlikely	The likelihood is reduced by: • The lead agency providing guidance and configuration recommendations during the onboarding process to enable security controls. A checklist has been developed as part of the onboarding pack. • An agency performing regular checks of the configuration against the recommendations provided by the lead agency. • Eightwire providing training to agency staff who will configure the service. The lead agency ensures this is completed as part of the onboarding process. It is an agency's responsibility for the ongoing training of new staff. • An agency creating tags for sensitive information. This will ensure an alert is generated when configuring a process that uses the tagged information. • A one-time code that must be provided to the recipient by the person setting up the sharing agreement. This code is sent out-of-band of the sharing email. The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. Note that all organisations must be approved by Eightwire before being granted access to the Data Exchange. It is not possible for a malicious person to self-register a new organisation and start participating in sharing agreements, without first being approved by Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR03	**Malware is distributed via the Data Exchange:** Eightwire (the vendor), an Agency or NGO intentionally or inadvertently shares malware or malicious commands through the Data Exchange. This may result in the infection of an Agency/NGO server, leading to loss or compromise of data, unavailability of systems and reputational damage. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • An agency that is configured to use the end to end file transfer feature inadvertently shares an infected PDF file through the Data Exchange. The PDF file is opened by the recipient and malware is automatically downloaded. The malware is cryptoware or ransomware that leads to information on file shares being made unavailable, with ransom demands being made to "release" the data. • A spreadsheet with a malicious macro is shared via the Data Exchange to an organisation that retains the same spreadsheet format. Upon opening the spreadsheet, the macro is executed and is used to download malware to the device. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • C08. Security Awareness (L) • C16. Management of Privileged Access (L) • **C31. Malware Protection (agency systems) (L/C)** • C32. Backup and Restore (agency systems) (C) • **C40. Security of Network Services (L/C)** • **C44. Firewalls** (L/C) • **C54. Information Security Incident Management (C)** • **SC07. Data Level Transfer Only (disable folder transfer unless explicitly required) (L)** **Lead Agency Responsibility** • C50. Contractual Agreements and SLA (with Eightwire to define reporting requirements) (L) • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C31. Malware Protection (L/C)** • C32. Backup and Restore (C) • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • C54. Information Security Incident Management (C) • **SC07. Data Level Transfer Only (disable file transfer unless explicitly required) (L)** • **SC08. Service Reporting (report of accounts <u>using</u> file transfer) (L)**	**MEDIUM** Major / Rare		**MEDIUM** Major / Rare	Subscribers that have enabled the folder transfer capability within the Data Exchange are susceptible to this risk. Folder transfer is disabled by default and can only be enabled by Eightwire. The likelihood is reduced by: • An agency installing and maintaining malware protection software on all their systems. • Eightwire scanning all files transferred via the Data Exchange for known malware and preventing their transfer if malware is detected. This is done to protect the Data Exchange platform. • The Data Exchange only transferring "data" rather than full files. • An agency installing the agent server in an isolated network and configuring firewall policy to only permit the sources, destination and services required to deliver the service. • Only enabling folder transfer if required. • Eightwire providing the lead agency with regular reports of agencies that are using the file transfer capability. The consequence is reduced by: • Agencies and Eightwire being able to detect Malware before it is executed. • An agency ensuring that their incident response processes consider a security incident that impacts the Data Exchange. • An agency installing the agent server in an isolated network and configuring firewall policy to only permit the sources, destination and services required to deliver the service. This will limit the ability of any malware to propagate. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR04	**Vendor viability:** Eightwire is no longer able to operate the Data Exchange platform, or go through a restructure or sale of business, meaning that security updates and support are no longer available. This may result in the Data Exchange being permanently unavailable or data being stolen or compromised due to unpatched vulnerabilities. **This may result in:** • Agency processes being interrupted or becoming unavailable for a prolonged period. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • Eightwire shutdown their business as it is not financially viable to continue to operate. The Data Exchange is handed over to a third party who do not have the expertise to operate and maintain it, and the platform becomes unreliable and susceptible to security incidents. • The lead agency is unable to obtain funding for the service beyond June 2021, and subscribing agencies are unwilling to commit to the platform without this funding. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** • C56. Business Continuity Plan (C) **Lead Agency Responsibility** • **C49. Due Diligence (L)** • **C51. Exit Strategy (L/C)** **Eightwire Responsibility** *No controls identified.*	**Medium** Major / Rare		**Medium** Major / Rare	The likelihood is reduced by: • The vendor's proven track record. The consequence is reduced by: • An agency documenting and testing a business continuity plan to ensure agency processes can continue to operate should the Data Exchange not be available.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR05	**The Data Exchange contains a vulnerability that can be exploited:** The Data Exchange agent, web application, "smart pipe" or underlying infrastructure has a security vulnerability. This may result in attackers stealing or compromising data that is being shared by Agencies or NGOs, or making the service unavailable. **This may result in:** • Agency information being disclosed to an unauthorised party. • Agency information is corrupted or modified by unauthorised party. • Stakeholders lose confidence in the system. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A critical vulnerability is discovered in Microsoft Internet Information Services (IIS) and Eightwire do not patch before an exploit is published. A malicious person searches the internet for unpatched systems and uses the published exploit to compromise the web server host and obtain access to authentication keys, gaining unauthorised access to the Data Exchange. • Eightwire update the Data Exchange software and introduce a vulnerability as the code is not reviewed or security tested. A motivated attacker exploits the weakness to obtain unauthorised access to an agency's environment, where they are able to setup a data sharing process to exfiltrate agency information. • An authorised user of the Data Exchange exploits a vulnerability to escalate their privileges or can access another customers tenancy. This leads to unauthorised access to agency information. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** • C50. Contractual Agreements and SLA (with Eightwire) (L) • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • C32. Backup and Restore (C) • C33. Event Logging (L/C) • C35. Clock Synchronisation (C) • **C38. Patch and Vulnerability Management (L)** • **C39. Hardening of Systems, Network Devices and Applications (L)** • **C40. Security of Network Services (L/C)** • **C44. Firewalls (L/C)** • C45. Web Application Firewall (L) • **C48. Secure Application Development (L)** • **C54. Information Security Incident Management (C)** • C59. Independent Review of Information Security (L) • **C67. Penetration testing and vulnerability scanning (L)** • **SC02. Non-persistent data transfer (L/C)**	**MEDIUM** Major / Unlikely		**MEDIUM** Major / Unlikely	The likelihood is reduced by: • Eightwire patching and maintaining the server operating systems and applications. • Eightwire hardening the servers by removing unnecessary services and functionality. • Eightwire isolating servers from one another using network isolation and associated firewall rules to prevent lateral movement within the environment. • Eightwire implementing the recommendations from the completed penetration test. • Secure code development, as verified by the lack of vulnerabilities confirmed by the completed penetration test. Source code was provided to support the penetration test. • The service securely storing information as it is being processed, and securely removing it once the transfer is complete. The consequence is reduced by: • An agency ensuring that their incident response processes consider a security incident that impacts the Data Exchange. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire. • The service securely storing information as it is being processed, and securely removing the information once the transfer is complete.

SR06	**Agency data is accidentally shared with a non-authorised party:** An Agency/NGO shares data outside of what has been agreed by MoUs, either intentionally or accidentally (i.e. misconfiguring the web application). This may result in the unauthorised disclosure, loss or modification of sensitive or personal information, and lead to severe reputational damage for SWA and the Sharing Agency. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. **Example Scenario(s):** • An agency administrator accidentally shares information with an unauthorised party as they enter the wrong email address when configuring a data sharing process. The unauthorised party installs the agent and configures it to save data to a CSV file and uses the information to discredit the agency. • An agency administrator accidentally shares information with an unauthorised party and realises their error. The transfer may be paused, and then inadvertently resumed, without the intention to resume the transfer, and information is corrupted or lost. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C07. Role-Based Training (L)** • C16. Management of Privileged Access (L) • **C19. Access Control (configure) (L)** • C26. Standard Operating Procedures (L) • **C54. Information Security Incident Management (C)** • **C62. Security Tests and Controls Audit (L)** • **SC03. Acceptable Data Assurance (configure) (L)** • SC09. Memorandum of Understanding (L) **Lead Agency Responsibility** • **C07. Role-Based Training (L)** • **C26. Standard Operating Procedures (onboarding process) (L)** **Eightwire Responsibility** • C19. Access Control (implement capability) (L) • C26. Standard Operating Procedures (develop for agencies) (L) • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • SC03. Acceptable Data Assurance (implement capability) (L) • SC09. Memorandum of Understanding (provide the ability to record agreements within the DX) (L) • **SC11. Sharing One-time Code**	**MEDIUM** Major / Unlikely		**MEDIUM** Major / Unlikely	The likelihood is reduced by: • The lead agency providing guidance and configuration recommendations during the onboarding process to enable security controls. A checklist has been developed as part of the onboarding pack. • An agency configuring access controls so that users are only provided with the level of access required for them to complete their role. • An agency performing regular checks of the configuration against the recommendations provided by the lead agency, and regularly reviewing configured sharing agreements. • Eightwire providing training to agency staff who will configure the service. The lead agency will ensure this is completed as part of the onboarding process. It is an agency's responsibility for the ongoing training of new staff. • An Agency creating tags for sensitive information. This will ensure an alert is generated when configuring a process that uses the tagged information. • A one-time code that must be provided to the recipient by the person setting up the sharing agreement. This code is sent out-of-band of the sharing email. The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. Note that all organisations must be approved by Eightwire before being granted access to the Data Exchange. It is not possible for a malicious person to self-register a new organisation and start participating in sharing agreements, without first being approved by Eightwire.
SR07	**Access controls are not correctly configured:**	**MEDIUM**	**Subscribing Agency Responsibility**	**LOW**		**LOW**	Note that if a user account is compromised an attacker would assume the identity and

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
	If there is a lack of proper user access management for authorised users, this could lead to a user seeing information they should not have access to or being able to perform tasks they should not be able to. This could result in a client privacy breach, a significant disruption to the service, or corruption of the information. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • For example, an agency by default sets up users as Account or Project administrators when onboarded. This results in too many administrators and leads to service disruptions due to changes being made in a non-controlled manner. • Account administrators add themselves or others to projects, without the authorisation of the information owner. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	Moderate / Possible	• **C07. Role-Based Training (L)** • **C14. Access Control Management (L)** • **C16. Management of Privileged Access (L)** • **C19. Access Control (configure) (L)** • C26. Standard Operating Procedures (L) • **C54. Information Security Incident Management (C)** • **C62. Security Tests and Controls Audit (L)** **Lead Agency Responsibility** • **C07. Role-Based Training (L)** • **C26. Standard Operating Procedures (onboarding process) (L)** • C50. Contractual Agreements and SLA (with Eightwire to define reporting requirements) (L) **Eightwire Responsibility** • C19. Access Control (implement capability) (L) • C26. Standard Operating Procedures (develop for agencies) (L) • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • **SC08. Service Reporting (report of account administrators vs total users for an account) (L)** • SC11. Sharing One-time Code	Minor / Unlikely		Minor / Unlikely	privileges of the compromised account. This risk is assessed based on an authorised user of the platform being granted excessive permission or rights. The likelihood is reduced by: • The lead agency providing guidance and configuration recommendations during the onboarding process to enable security controls. A checklist has been developed as part of the onboarding pack. • An agency configuring access controls so that users are only provided with the level of access required for them to complete their role. • An agency restricting the number of users that are granted administrator privileges. • An agency performing regular checks of the configuration against the recommendations provided by the lead agency. • Eightwire providing training to agency staff who will configure the service. The lead agency will ensure this is completed as part of the onboarding process. It is an agency's responsibility for the ongoing training of new staff. • Eightwire providing the lead agency with regular reports of agencies that have not configured control recommendations (for this risk, a report of account administrators vs total users for an account). The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR08	**Log information is not available to support a security investigation:** If a security incident occurs, Agencies/NGOs will be unable to investigate due to poor or unavailable logs, or ineffective cooperation between parties. This may result in the service being taken offline, or reputational damage to parties that were involved in the breach. **This may result in:** • Agency processes being interrupted or becoming unavailable for a prolonged period. • Increased workloads to investigate and resolve incidents. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A malicious person obtains access to an agency's Data Exchange environment and can exfiltrate agency data. The agency discovers the compromise however is unable to determine how long the service has been comprised, and to what extent, as detailed log files are not available. The agency ceases all operations through the Data Exchange. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**MEDIUM** Moderate /Possible	**Subscribing Agency Responsibility** • C54. Information Security Incident Management (C) **Lead Agency Responsibility** • C50. Contractual Agreements and SLA (with Eightwire to define logging requirements) (L) • C54. Information Security Incident Management (C) **Eightwire Responsibility** • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • C50. Contractual Agreements and SLA (with vendors) (L) • C54. Information Security Incident Management (C)	**VERY LOW** Minor / Rare		**VERY LOW** Minor / Rare	Please note that this risk has been assessed in the context of logging information not being available and does not assess the impact of the actual security incident. Security incidents are captured by other risks. The likelihood is reduced by: • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. The consequence is reduced by: • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale

SR09	**A malicious administrator performs an undesirable action:**
	A malicious or compromised Eightwire or agency administrator abuses their privileges and deliberately makes a configuration change to the solution that has an undesirable outcome.
	This may lead to the solution becoming unavailable, or exploited resulting in the unauthorised disclosure, modification, or loss of Sharing Agency data.
	
	This may result in:
	• Agency information being disclosed to an unauthorised party.
	• Agency processes being interrupted or becoming unavailable for a prolonged period.
	• Reputational damage to the agency.
	• Reputational damage to the Social Wellbeing Agency.
	
	Example Scenario(s):
	• An administrator who is under financial pressure, or with links to organised crime, is coerced into making a configuration change that provides unauthorised access to data transferred through the DX. This is achieved by creating a new user account for a subscribing agency and providing the account to an external entity. The account is used to:
	  ○ download a new agent.
	  ○ configure a new datastore.
	  ○ configure an associated process.
	  ○ exfiltrate agency data.
	• An Eightwire administrator with malicious intent uses the impersonate feature (used for valid support purposes) to impersonate an agency user and complete the above steps.
	
	Affects:
	☒ Confidentiality, ☒ Integrity, ☒ Availability
		HIGH
		Severe / Unlikely
			Subscribing Agency Responsibility
			• **C06. Screening (L)**
			• C16. Management of Privileged Access (L)
			• C54. Information Security Incident Management (C)
			
			Lead Agency Responsibility
			• C54. Information Security Incident Management (C)
			
			Eightwire Responsibility
			• **C06. Screening (L)**
			• C16. Management of Privileged Access (L)
			• **C33. Event Logging, Alerting and Auditing (L/C)**
			• C35. Clock Synchronisation (C)
			• C54. Information Security Incident Management (C)
				MEDIUM
				Major / Rare
					Eightwire Responsibility
					• **C06. Screening (L)**
					  ○ Ministry of Justice background checks have not been completed for all Eightwire staff.
						MEDIUM
						Major / Rare
							The likelihood is reduced by:
							• Ministry of Justice checks having been completed for all but two Eightwire staff.
							• An agency performing security vetting of staff before they are granted access to the service.
							
							The consequence is reduced by:
							• Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR10	**Configuration information is compromised and used to obtain access to the platform:** Configuration details are stolen for the web application or an associated database/server by being captured in transit or are obtained from the agent or server configuration. This may result in an attacker gaining access to an Agency's Data Exchange web application account or database and stealing information. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • Within the Data Exchange, a database connection is established over an untrusted network (such as the internet). A malicious person can intercept traffic traversing this network and obtain database credentials and can use these credentials to connect directly to the database. Once connected to the database, they can view, modify or delete service information. • An attacker exploits a vulnerability in the Data Exchange and can compromise a host, gaining full administrator level access to the operating system. The attacker accesses configuration files or the registry to obtain credentials to other system components and is able to use these credentials to obtain access to an agency's Data Exchange environment. • A malicious person obtains access to the server where the agent is installed and can view the Conductor Agent configuration file that contains database credentials. They use this information to connect to the database to gain access to information. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** • **C15. User and Device Access Management (L)** • **C21. Encryption of Data in Transit (consider SSL inspection) (L/C)** • C23. Cryptographic Key Management (consider SSL inspection on agency proxy, if enabled) (L) • C33. Event Logging, Alerting and Auditing (L/C) • **C39. Hardening of Systems, Network Devices and Applications (L)** • C40. Security of Network Services (L/C) • C44. Firewalls (L/C) • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C15. User and Device Access Management (L)** • **C21. Encryption of Data in Transit (L/C)** • **C23. Cryptographic Key Management (L)** • C33. Event Logging, Alerting and Auditing (L/C) • C35. Clock Synchronisation (C) • **C39. Hardening of Systems, Network Devices and Applications (L)** • C40. Security of Network Services (L/C) • C44. Firewalls (L/C) • **C54. Information Security Incident Management (C)** • C67. Penetration testing and vulnerability scanning (L) • SC12. Mask Data Store Credentials (L)	**MEDIUM** Major / Rare	• C22. Encryption of Data at Rest (protect configuration files) (L/C)	**MEDIUM** Major / Rare	The likelihood is reduced by: • An agency hardening the server where the agent is installed, and restricting access to the server, specifically to the location the agent configuration file is stored. • An agency ensuring connections from the agent or from the Data Exchange (in the case of cloud only data stores) to their data stores are over trusted networks or are encrypted. • The agent configuration file being encrypted. • Eightwire hardening the servers by removing unnecessary services and functionality, and by restricting access to the servers. • Eightwire protecting the private keys used to encrypt data, by restricting access to the keys. • All data transfers to the Data Exchange being encrypted using TLSv1.2. The consequence is reduced by: • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. • Encrypting information in transit and at rest. If information is obtained it would be unusable as it is in an encrypted format. • An agency ensuring that their incident response processes consider a security incident that impacts the Data Exchange. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR11	**The Privacy Act is breached:** If the service fails to meet its obligations as per the Privacy Act, then the Privacy Commissioner may investigate client complaints relating to breaches. This may result in reputational damage to the Sharing Agency. **This may result in:** • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • An agency uses the service to receive types of personal information that are not required for the business processes supported by the Data Exchange. A security incident occurs, and all information processed by the Data Exchange for the agency is compromised. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • C07. Role-Based Training (reason for sharing field) (L) • **SC03. Acceptable Data Assurance (configure) (L)** • **SC04. Privacy Impact Assessment (L/C)** • SC09. Memorandum of Understanding (L) **Lead Agency Responsibility** • C07. Role-Based Training (L) • C26. Standard Operating Procedures (onboarding process) (L) • **SC04. Privacy Impact Assessment (L/C)** **Eightwire Responsibility** • **SC03. Acceptable Data Assurance (enable capability) (L)** • SC09. Memorandum of Understanding (provide the ability to record agreements within the DX) (L)	**MEDIUM** Major / Unlikely		**MEDIUM** Major / Unlikely	The likelihood is reduced by: • An Agency creating tags for personal information. This will ensure an alert is generated when configuring a process that uses the tagged information. • An agency completing a privacy impact assessment to understand their obligations for the protection of personal information, prior to configuring a sharing agreement. • A requirement to complete a "reason for sharing field" when creating a process to share information. • The lead agency seeking guidance on the requirement to complete an updated privacy impact assessment based on the changes made since the last assessment. An updated privacy impact assessment is <u>not</u> required. The consequence is reduced by: • An agency completing a privacy impact assessment to understand their obligation for the protection of personal information, prior to configuring a sharing agreement. This manages the consequence as only information they are permitted to share is shared, reducing the consequence should information be compromised.

SR12	**Information is intercepted in transit, leading to unauthorised access:** If the data transferred between the agent and the Data Exchange is intercepted, a malicious third party could view or change data in transit. This may result in lost or compromised information, service disruption, a reduced level of service to Agencies/NGOs, and damage to the Ministry's reputation as a secure/trusted service provider. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. • Stakeholders losing confidence in the system. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • An internet service provider (ISP) network administrator with malicious intent captures network traffic as it traverses their network and can view agency information as it enters or leaves the Data Exchange. The information is captured and made publicly available or used for other malicious purposes. • An agency network administrator with malicious intent captures network traffic as it traverses the agency network and can view agency information as it is sent to and from the Data Exchange. The information is captured and made publicly available or used for other malicious purposes. • A malicious person obtains the web server certificate and uses the certificate to unencrypt information that they have been able to capture as it is in transit. The information is made publicly available or used for other malicious purposes. • An agency uses a proxy server to connect to the internet and perform HTTPS interception to allow encrypted content to be inspected. An administrator of the proxy service takes advantage of their access permissions to capture network traffic on the proxy and view or modify agency information as it is sent to and from the Data Exchange. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** • **C21. Encryption of Data in Transit (consider SSL inspection on agency proxy, if enabled) (L/C)** • **C23. Cryptographic Key Management (consider SSL inspection on agency proxy, if enabled) (L)** • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C21. Encryption of Data in Transit (L/C)** • **C23. Cryptographic Key Management (L)** • **C54. Information Security Incident Management (C)** • C67. Penetration testing and vulnerability scanning (L)	**VERY LOW** Minor / Rare		**VERY LOW** Minor / Rare	The likelihood is reduced by: • Eightwire protecting the private keys used to encrypt data, by restricting access to the keys. • All data transfers to the Data Exchange being encrypted using TLSv1.2. • An agency considering their use of proxy services, their use of SSL intercept and inspection on the proxy, and the protection of private keys used for inspection. The consequence is reduced by: • Encrypting information in transit. If information is obtained it would be unusable as it is in an encrypted format. • An agency ensuring that their incident response processes consider a security incident that impacts the Data Exchange. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR13	**Incorrect or invalid data is shared:** An Agency or NGO shares incorrect or invalid data through the Data Exchange agent. This may result in another party losing or overwriting valid information or receiving incorrect or corrupt data. **This may result in:** • Agency processes are interrupted or become unavailable for a prolonged period. • Reputational damage to the agency. **Example Scenario(s):** • The autoscan feature used to keep datastores updated incorrectly changes the metadata type, leading to data integrity issues. This results in incorrect data being relied upon by an Agency or their partners. • An internal agency process fails, and incorrect data is shared via the Data Exchange. The receiving party processes the data and relies on the incorrect data to make business decisions or is unable to use the data as it does not meet the expected format of data to be received. **Affects:** ☐ Confidentiality, ☒ Integrity, ☐ Availability	**MEDIUM** Moderate / Possible	**Subscribing Agency Responsibility** • **C07. Role-Based Training (L)** • C16. Management of Privileged Access (L) • C19. Access Control (configure) (L) • **SC05. Destination Update Options (enable) (L/C)** **Lead Agency Responsibility** • **C07. Role-Based Training (L)** • **C26. Standard Operating Procedures (onboarding process) (L)** **Eightwire Responsibility** • C19. Access Control (implement capability) (L) • **C26. Standard Operating Procedures (for agency use) (L)** • **SC05. Destination Update Options (implement capability) (L/C)**	**LOW** Minor / Unlikely		**LOW** Minor / Unlikely	The likelihood is reduced by: • The lead agency providing guidance and configuration recommendations during the onboarding process to enable security controls. A checklist has been developed as part of the onboarding pack. • Eightwire providing training to agency staff who will configure the service. The lead agency will ensure this is completed as part of the onboarding process. It is an agency's responsibility for the ongoing training of new staff. • An agency configuring the destination action on a process group to control if information is overwritten, merged, appended, or written to a new location. • An agency configuring the column matching threshold on a process to the maximum setting. This will "abort a load if anything other than the most minor changes are found". The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. • An agency configuring the destination update options on a receiving data store to control if information is overwritten, merged, appended, or written to a new location.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR14	**Data is corrupted due to the failure of the Data Exchange or a supporting network:** Data is corrupted or the connection is dropped during a transfer between the agent and the Data Exchange. This may result in incorrect, incomplete or invalid data being transferred between parties. **This may result in:** • Reputational damage to the agency. **Example Scenario(s):** • The network connection is interrupted, or the Data Exchange experiences an outage during a data transfer between the Conductor agent and the Data Exchange. The data is corrupted or incomplete data is transferred, and the data is relied upon by the receiving party. **Affects:** ☐ Confidentiality, ☒ Integrity, ☐ Availability	**MEDIUM** Moderate / Unlikely	**Subscribing Agency Responsibility** • C07. Role-Based Training (L) • SC05. Destination Update Options (enable) (L/C) **Lead Agency Responsibility** • C07. Role-Based Training (L) • C26. Standard Operating Procedures (onboarding process) (L) **Eightwire Responsibility** • C26. Standard Operating Procedures (for agency use) (L) • **C46. Message Integrity (L/C)** • **C58. Fault Tolerance (L/C)** • SC05. Destination Update Options (implement capability) (L/C)	**VERY LOW** Minor / Rare		**VERY LOW** Minor / Rare	The likelihood is reduced by: • The Data Exchange performing integrity checks for information that is transferred. • The inherent reliability and fault tolerance within the AWS and Revera platforms. The consequence is reduced by: • The Data Exchange performing integrity checks for information that is transferred and halting the process if an issue is detected.
SR15	**A government or law enforcement agency demands access to information stored by the Data Exchange:** If NZ Police or Government, a foreign government or courts compel Eightwire, Revera or Amazon Web Services to share information stored in their cloud platform then client's privacy will be breached. **This may result in:** • Agency information being disclosed to an unauthorised party. • Stakeholders losing confidence in the system. **Example Scenario(s):** • A non-Government user of the Data Exchange is suspected of using the Data Exchange to transfer illegal material, and a court order is issued for Eightwire to release all information stored in the platform, including access keys for all customers. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**MEDIUM** Moderate / Unlikely	**Subscribing Agency Responsibility** • **SC06. Agency Data Restricted to NZ (enable) (L/C)** **Lead Agency Responsibility** *No controls identified* **Eightwire Responsibility** • C18. Password Management System (L) • **SC02. Non-persistent data transfer (L/C)** • **SC06. Agency Data Restricted to NZ (implement capability) (L/C)** • SC08. Service Reporting (report on number of law enforcement requests) (C)	**VERY LOW** Minor / Rare		**VERY LOW** Minor / Rare	This risk has been assessed based on the fact that agency data that is transferred by the Data Exchange is not stored by the Data Exchange. If information were to be released by Eightwire, the information would not be released publicly by the party that it is released to. The consequence and likelihood are reduced by: • An agency configuring the data store to use New Zealand hosted processing servers. • The Data Exchange not retaining information after it has been processed, and by securely deleting information once processed.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR16	**Backup data is not transmitted or stored securely:** Data stored by the Data Exchange and backed up by Eightwire is not appropriately protected while at rest or in transit. This can result in the unauthorised disclosure, modification and loss of classified information. **This may result in:** • Agency information being disclosed to an unauthorised party. • Stakeholders losing confidence in the system. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A malicious person uses a script to scan AWS storage buckets to find buckets that are publicly available. They stumble across the storage bucket that is used by Eightwire to archive system log files. They post the contents of the log files to pastebin or add the storage bucket to a list of publicly accessible buckets. The log files contain some sensitive information as when an error occur full data is written to log files for debug purposes. • Private keys used by the service are backed up alongside other configuration data and are stored in an AWS storage bucket. Access controls on the storage bucket are not correctly configured and a malicious person is able to obtain the keys and use them to access the Data Exchange directly or use them as part of a phishing campaign (in the case of web server certificates) to spoof Eightwire services. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Major / Possible	**Subscribing Agency Responsibility** *No controls identified* **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • C13. Media Sanitisation and Disposal (L) • C16. Management of Privileged Access (L) • **C17. Multi-Factor-Authentication (L)** • **C19. Access Control (L)** • **C21. Encryption of Data in Transit (L/C)** • **C22. Encryption of Data at Rest (Database) (L/C)** • **C23. Cryptographic Key Management (L)** • **C32. Backup and Restore (L/C)** • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • C39. Hardening of Systems, Network Devices and Applications (L) • C40. Security of Network Services (L/C) • C44. Firewalls (L/C) • **C54. Information Security Incident Management (C)** • **C59. Independent Review of Information Security (L)** • C67. Penetration testing and vulnerability scanning (L) • **SC02. Non-persistent data transfer (L/C)**	**VERY LOW** Minor / Rare	• **C22. Encryption of Data at Rest (Storage Buckets) (L/C)**	**VERY LOW** Minor / Rare	Agency data is not stored and backed up by the Data Exchange. Only meta data is backed up. This risk relates to metadata and configuration data only. The likelihood is reduced by: • Multi-factor authentication being enforced for all user access to the AWS environment. • Access control lists configured on the storage accounts used to store backup data. Public access is not permitted. • All data transfers to the storage account used for backups being encrypted in transit using TLSv1.2. • An independent review of the AWS environment being completed. The consequence is reduced by: • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. • Encrypting information in transit and at rest. If information is obtained it would be unusable as it is in an encrypted format. • An agency ensuring that their incident response processes consider a security incident that impacts the Data Exchange. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR17	**An infrastructure failure leads to the Data Exchange becoming unavailable:** The underlying infrastructure supporting the Data Exchange (AWS or Revera) becomes unavailable or unreliable. This may result in the Agencies or NGOs being unable to share data with each other. **This may result in:** • Agency processes being interrupted or becoming unavailable for a prolonged period. • Stakeholders losing confidence in the system. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • The datacentre in which the Data Exchange is hosted suffers a catastrophic equipment failure, and the Data Exchange is taken offline. • An individual component of the Data Exchange experiences a software failure or error, and the Data Exchange is not available, or does not process information on schedule. • Multiple new customers sign on to the Eightwire service and Eightwire do not increase capacity to cope with the demand. During a period of peak use the Data Exchange becomes unreliable and is unable to process agency data in a timely fashion. **Affects:** ☐ Confidentiality, ☐ Integrity, ☒ Availability	**MEDIUM** Moderate / Possible	**Subscribing Agency Responsibility** • C56. Business Continuity Plan (C) **Lead Agency Responsibility** • **C50. Contractual Agreements and SLA (with Eightwire) (L)** **Eightwire Responsibility** • **C29. Performance and Capacity Management (L/C)** • C32. Backup and Restore (C) • **C50. Contractual Agreements and SLA (with vendors) (L)** • C57. Disaster Recovery Plan (C) • **C58. Fault Tolerance (L/C)**	**LOW** Minor / Unlikely		**LOW** Minor / Unlikely	The likelihood is reduced by: • The service level agreements (SLAs) defined in the master services agreement. • The inherent reliability and fault tolerance within the AWS and Revera platforms. • The ability of the Data Exchange to direct requests to available processing servers. The consequence is reduced by: • The inherent reliability and fault tolerance within the AWS and Revera platforms. • The ability of the Data Exchange to direct requests to available processing servers. • Eightwire monitoring the performance of the Data Exchange and being able to add additional capacity if required.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR18	**A catastrophic event leads to the Data Exchange becoming unavailable:** If the service were unavailable, due to a natural disaster or some other catastrophic event for the period of 30 days, this would result in the Sharing Agency transmitting data using less efficient / legacy methods such as SFTP or IronKey. **This may result in:** • Agency processes being interrupted or becoming unavailable for a prolonged period. • Stakeholders losing confidence in the system. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A major earthquake impacts the Revera data centre and processing servers are unavailable to process agency data onshore. Agencies are required to find alternate methods to transfer data. **Affects:** ☐ Confidentiality, ☐ Integrity, ☒ Availability	**LOW** Moderate / Rare	**Subscribing Agency Responsibility** • **C56. Business Continuity Plan (C)** **Lead Agency Responsibility** • **C50. Contractual Agreements and SLA (with Eightwire) (L)** **Eightwire Responsibility** • **C32. Backup and Restore (C)** • **C50. Contractual Agreements and SLA (with vendors) (L)** • **C57. Disaster Recovery Plan (C)** • **C58. Fault Tolerance (L/C)**	**VERY LOW** Minor / Rare		**VERY LOW** Minor / Rare	The likelihood is reduced by: • The service level agreements (SLAs) defined in the master services agreement. • The inherent reliability and fault tolerance within the AWS and Revera platforms. • The ability of the Data Exchange to direct requests to available processing servers. The consequence is reduced by: • The inherent reliability and fault tolerance within the AWS and Revera platforms. • The ability of the Data Exchange to direct requests to available processing servers. • Eightwire regularly backing up the master database. • Eightwire being able to rebuild the service in an alternate location. • Eightwire testing the rebuild process. • An agency documenting and testing a business continuity plan to ensure agency processes can continue to operate should the Data Exchange not be available.
SR19	*Please note previous risk SR19 has been added as a scenario to risk SR06.*						
Risks from the 2020 Certification Below							

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR20	**IPv6 is enabled and not required, and network security controls can be bypassed:** An internet facing component of the service is compromised as IPv6 is enabled by default and many security controls are only configured to support IPv4. Alternatively, an internet facing host is compromised and the attacker can move laterally within the environment using IPv6, bypassing configured IPv4 security controls. The Data Exchange is compromised as a weakness is exposed, and an attacker can obtain access to agency information. **This may result in:** • Agency information being disclosed to an unauthorised party. • Agency processes being interrupted or becoming unavailable for a prolonged period. • Stakeholders losing confidence in the system. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A Windows server used to deliver the service has IPv6 enabled and is exposed to the internet as network security controls are only configured for IPv4. This allows an attacker to attempt remote access to the server using RDP and they obtain access due to a vulnerability or configuration weakness. The Data Exchange is compromised, and an attacker can obtain access to agency information. • An attacker can compromise the web service as it contains a vulnerability and obtains administrator (root) access to the server. From here the attacker can move laterally within the environment and access other servers as IPv6 is enabled on all servers, and IPv6 security controls are not configured. The Data Exchange is compromised, and an attacker can obtain access to agency information. **Affects:** ☒ Confidentiality, ☒ Integrity, ☒ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C39. Hardening of Systems, Network Devices and Applications (disable IPv6) (L)** • **C44. Firewalls (L/C)** **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C39. Hardening of Systems, Network Devices and Applications (disable IPv6) (L)** • C40. Security of Network Services (L/C) • C44. Firewalls (L/C) • **C54. Information Security Incident Management (C)** • C59. Independent Review of Information Security (L) • C67. Penetration testing and vulnerability scanning (L)	**MEDIUM** Major / Rare		**MEDIUM** Major / Rare	The likelihood is reduced by: • Eightwire disabling IPv6 on all servers. • Eightwire not allocating an IPv6 address space to subnet configuration. • An agency disabling IPv6 on the agent server, unless explicitly required. • An agency configuring firewall policy to filter IPv6 traffic. The consequence is reduced by: • An agency ensuring that their incident response processes consider a security incident that impacts the Data Exchange. • An agency configuring firewall policy to filter IPv6 traffic. This may help to contain a security incident. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR21	**Denial of Service attack:** A malicious party performs a sustained Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack against the Data Exchange, leading to it being unavailable or unreliable for a prolonged period. **This may result in:** • Subscriber processes are interrupted or become unavailable for a prolonged period. • Reputational Damage to the Social Wellbeing Agency. **Example Scenario(s):** • A hacktivist, hacktivist group, or foreign government launches an attack against multiple Government services, one of which is the DX. This leads to the service being unavailable for an extended period. **Affects:** ☐ Confidentiality, ☐ Integrity, ☒ Availability	**MEDIUM** Moderate/ Unlikely	**Subscribing Agency Responsibility** • C56. Business Continuity Plan (C) **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C41. Denial of Service (DoS) Protection (L/C)** • **C54. Information Security Incident Management (C)**	**LOW** Minor / Unlikely		**LOW** Minor / Unlikely	The likelihood is reduced (but not substantially) by: • The default AWS DoS and DDoS protections. • The Eightwire process to enable advanced DoS and DDoS protection services. The consequence is reduced by: • The default AWS DoS and DDoS protections. • The Eightwire process to enable advanced DoS and DDoS protection services. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR22	**DNS is compromised:** A malicious person can access the DNS registrar portal, or the DNS hosting portal, for the domain eight-wire.com, as they have exploited a vulnerability within the platform, or have obtained valid credentials. This allows them to: • Modify MX records to redirect password reset emails for Eightwire system administrators. • Redirect Data Exchange subscribers to spoofed services. • Send phishing emails to system users. • Create web certificates for spoofed services to make them appear legitimate (many certificate providers allow customers to validate the domain via DNS TXT records). • Remove DNS records. • Transfer DNS records and therefore the control of DNS records to a malicious party. **This may result in:** • Agency information being disclosed to an unauthorised party. • Agency processes being interrupted or becoming unavailable for a prolonged period. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • Eightwire use a shared account to manage DNS records and the configured password is used across multiple services, one of which is compromised and has its password store breached and leaked. An attacker obtains the compromised username and password, and after performing a DNS lookup to determine the DNS hosting provider for the eight-wire.com domain, successfully logs in and changes DNS records. **Affects:** ☒ Confidentiality, ☐ Integrity, ☒ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** No controls identified **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C17. Multi-Factor-Authentication (DNS provider) (L)** • C49. Due Diligence (of DNS provider) (L) • **C54. Information Security Incident Management (C)**	**MEDIUM** Major / Rare		**MEDIUM** Major / Rare	The likelihood is reduced by: • Enforcing multi-factor authentication for administrator access to the DNS portal. The consequence is reduced by: • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR23	**Agent credentials are compromised:** A malicious person obtains access to an agent's authentication key and can connect to the DX to compromise and Agency's transfer through the DX. **This may result in:** • Agency information being disclosed to an unauthorised party. • Stakeholders losing confidence in the system. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A system on which the Conductor agent is installed is compromised, and a malicious person can obtain the authentication keys. The keys are used to authenticate to the Data Exchange and access agency information. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C07. Role-Based Training (L)** • C19. Access Control (protect installer) (L) • C33. Event Logging, Alerting and Auditing (L/C) • C39. Hardening of Systems, Network Devices and Applications (L) • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** • **C26. Standard Operating Procedures (onboarding process) (L)** • C50. Contractual Agreements and SLA (with Eightwire to define reporting requirements) (L) • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C26. Standard Operating Procedures (for agency use) (L)** • C33. Event Logging, Alerting and Auditing (L/C) • C35. Clock Synchronisation (C) • **C54. Information Security Incident Management (C)** • **SC10. Agent Authentication (L)**	**MEDIUM** Major / Rare		**MEDIUM** Major / Rare	The likelihood is reduced by: • The agent authentication mechanism. The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. *Note that agent authentication was introduced following the 2020 certification. The authentication key is no longer embedded in the installer.*

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR24	**Accidental or inadvertent misconfiguration (Eightwire):** An Eightwire administrator accidentally makes a configuration or code change that introduces a weakness, or inadvertently makes a change that has unintended consequences. The weakness is exploited by a malicious person to access and disclose agency information. **This may result in:** • Subscriber information being disclosed to an unauthorised party. • Subscriber processes are interrupted or become unavailable for a prolonged period. • Reputational Damage to the Subscriber. • Reputational Damage to the Social Wellbeing Agency. **Example Scenario(s):** • A new staff member at Eightwire is provided with full administrator access to the Data Exchange. The staff member is provided with minimal training and to resolve an issue makes a configuration change that has unintended consequences. This weakens the security posture of the Data Exchange for all agencies. **Affects:** ☒ Confidentiality, ☐ Integrity, ☒ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** *No controls identified* **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • C07. Role-Based Training (L) • C16. Management of Privileged Access (L) • C26. Standard Operating Procedures (L) • **C28. Change Management (L)** • C32. Backup and Restore (C) • **C33. Event Logging, Alerting and Auditing (L/C)** • C35. Clock Synchronisation (C) • C37. Release Management (L) • C48. Secure Application Development (L) • **C54. Information Security Incident Management (C)** • C59. Independent Review of Information Security (L) • C67. Penetration testing and vulnerability scanning (L)	**MEDIUM** Major / Rare		**MEDIUM** Major / Rare	The likelihood is reduced by: • Eightwire providing training to staff who will configure and support the service. • Eightwire change control processes that ensure all changes are documented and tested before implementation. The consequence is reduced by: • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire. • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR25	**A session token is compromised and used to obtain unauthorised access:** A malicious person compromises a portal user's device or browser due to a configuration weakness or known vulnerability and can steal session tokens as the user has not logged out or the session tokens are not invalidated. This allows the attacker to gain access to an Agency's Data Exchange web application account and steal information that is shared using the Data Exchange. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. **Example Scenario(s):** • A device used by an agency Data Exchange administrator is infected with malware and an attacker can obtain session keys from the browser. Using the session keys, an attacker is able to logon to the Data Exchange web portal, download the agent and exfiltrate agency data. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** • **C19. Access Control (L)** • **C39. Hardening of Systems, Network Devices and Applications (L)** • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** *No controls identified* **Eightwire Responsibility** • C48. Secure Application Development (L) • **C67. Penetration testing and vulnerability scanning (L)**	**MEDIUM** Major / Rare		**MEDIUM** Major / Rare	The likelihood is reduced by: • Agencies ensuring that the security posture of the devices used to access the Data Exchange web portal is maintained. • Agencies restricting access to the devices used to access the Data Exchange web portal. • The penetration test identifying the issue and requiring compensating controls to be implemented. • The short timeframe that the session tokens remain valid for. • The token being removed from a user's browser after logging out. The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR26	**A cloud service access key is compromised** An agency establishes a connection to a cloud only data source and the access key is compromised as it is not stored securely or is intercepted in transit. This allows an attacker to obtain unauthorised access to information in the cloud data store. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. **Example Scenario(s):** • An authorised user of the Data Exchange can obtain credentials to a cloud only datastore as they are stored in clear text. They use this information to connect directly to the datastore and use the information for malicious purposes. • The Data Exchange establishes a connection to a cloud only datastore and the communication are not encrypted. This allow a malicious person to intercept the traffic and obtain credentials for the cloud only datastore, providing them with access to the data store. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**HIGH** Severe / Possible	**Subscribing Agency Responsibility** • **C06. Screening (L)** • C07. Role-Based Training (L) • **C21. Encryption of Data in Transit (L/C)** • **C23. Cryptographic Key Management (secure storage of keys) (L)** • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** • C07. Role-Based Training (L) • C26. Standard Operating Procedures (onboarding process) (L) • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C21. Encryption of Data in Transit (L/C)** • **C26. Standard Operating Procedures (develop for agencies) (L)** • C33. Event Logging, Alerting and Auditing (L/C) • C35. Clock Synchronisation (C) • **C54. Information Security Incident Management (C)** • SC12. Mask Data Store Credentials (L)	**MEDIUM** Major / Unlikely		**MEDIUM** Major / Unlikely	The likelihood is reduced by: • An agency performing security vetting of staff before they are granted access to the service. • An agency ensuring any connections to cloud only data stores are encrypted using approved cryptographic algorithms and protocols. • An agency protecting secret keys used to connect to cloud only datastores. The consequence is reduced by: • Logging and auditing within the Data Exchange. Logging and auditing are configured to capture all events and will support an investigation to determine the extent of a security incident. • Encrypting information in transit. If information is obtained it would be unusable as it is in an encrypted format.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR27	A password reset email is intercepted and a malicious person can reset a users' password to obtain access to the Data Exchange. The malicious person configures data sharing to exfiltrate agency data, and then releases it on the internet. **This may result in:** • Agency information being disclosed to an unauthorised party. • Reputational damage to the agency. • Reputational damage to the Social Wellbeing Agency. **Example Scenario(s):** • A malicious email administrator within an agency or at an email service provider sets up a mail rule to forward password reset emails to their own mailbox. They then reset the password for a Data Exchange user and login to set up a process to exfiltrate agency data. **Affects:** ☒ Confidentiality, ☐ Integrity, ☐ Availability	**HIGH** Severe / Unlikely	**Subscribing Agency Responsibility** • C08. Security Awareness (L) • **C17. Multi-Factor-Authentication (enable) (L)** • **C54. Information Security Incident Management (C)** **Lead Agency Responsibility** • **C54. Information Security Incident Management (C)** **Eightwire Responsibility** • **C17. Multi-Factor-Authentication (implement capability and enforce MFA for password resets) (L)** • **C21. Encryption of Data in Transit (enable opportunistic TLS on outgoing email relays) (L/C)** • C33. Event Logging, Alerting and Auditing (L/C) • C35. Clock Synchronisation (C) • **C54. Information Security Incident Management (C)** • **SC01. Email Protection (L)**	**MEDIUM** Major / Rare	• SC13. Timeout Password Reset Links (L)	**MEDIUM** Major / Rare	The likelihood is reduced by: • An agency enabling multi-factor authentication within the web portal to protect against scenarios where an attacker has been able to obtain a user's credentials. • Eightwire configuring TLS for email, for the email paths that they control. The consequence is reduced by: • An agency ensuring that their incident response process considers a security incident that impacts the Data Exchange. • The lead agency information security incident response plan for the Data Exchange. This plan is shared with Eightwire. • Encrypting emails in transit (where under the control of Eightwire). If information is obtained it would be unusable as it is in an encrypted format. • *Although the password reset link does not expire, if an account has multi-factor authentication enabled it is not possible for an attacker to use a password they have reset to access the Data Exchange.*

Appendix 2 – Controls

The table below provides details of the controls relied upon in the risk assessment above, the results of assessment activities to determine whether key controls are effective, and any agreed remediation activities where controls are not effective. The details of the control assessment activities, including why certain controls were not selected for assessment, can be found in the Control Assessment Report.

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
C01.	Information Security Policies		Not Used	
C02.	Information Security Governance		Not Used	
C03.	Segregation of Duties		Not Used	
C04.	Mobile Device Policy		Not Used	
C05.	Human Resource Security		Not Used	
C06.	Screening	As of 11/11/22 there are two Ministry of Justice (MoJ) checks that have not been completed for Eightwire staff members. All other checks confirm there are no convictions.	Partially Effective	Ministry of Justice background checks (or overseas equivalent) have not been completed for all Eightwire staff. **Remediation agreed with Responsible Manager** Once Ministry of Justice background checks (or overseas equivalent) have been completed for all Eightwire staff (two outstanding and currently being processed), Eightwire to report to the lead agency the outcome. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023
C07.	Role-Based Training	See Control Assessment Report for more details.	Effective	
C08.	Security Awareness	See Control Assessment Report for more details.	Effective	
C09.	Asset Lifecycle Management		Not Used	
C10.	Documentation		Not Used	
C11.	Information Lifecycle Management		Not Used	
C12.	Information Classification		Not Used	
C13.	Media Sanitisation and Disposal		Not Assessed (Not Key Control)	

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
C14.	Access Control Management		Not Assessed (Agency Control)	
C15.	User and Device Access Management		Not Assessed (Agency Control)	
C16.	Management of Privileged Access	See Control Assessment Report for more details.	Effective	
C17.	Multi-Factor-Authentication	See Control Assessment Report for more details.	Effective	
C18.	Password Management System	The password policies configured for the Conductor Web Portal and for administrators logging onto the servers meet the password requirements of the NZISM. The password policy in AWS and in GitHib does not meet the requirements of the NZISM, however the password policy cannot be modified.	Partially Effective	The password policy in AWS and in GitHub does not meet the requirements of the NZISM, however the password policy cannot be modified. It is recommended that Eightwire provide training to staff on the secure selection and storage of passwords, including the use of a secure password safe. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023
C19.	Access Control	See Control Assessment Report for more details.	Effective	
C20.	Cryptographic Policy		Not Used	

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
C21.	Encryption of Data in Transit	TLSv1.2 is configured and enforced for all Data Exchange endpoints accessible via HTTPS. Database connections are also encrypted. The AWS configuration review identified S3 storage buckets that do not enforce transport layer encryption on HTTP connections, however these buckets are blocked from public HTTP/S access, and are only accessed by other internal resources in AWS. It is a best practice to set this HTTPS condition on bucket policies regardless, and Eightwire do have this on their security improvement backlog. Connections between the load balancers and the containers are encrypted for the agent controller and for the AWS hosted processing servers, over which the actual data transfer occurs. Connections between the load balancers and the containers are not encrypted for the following services: • Conductor - main web portal • API - API services for Conductor site • Batch Controller - internal orchestration service for allocating jobs to processors However, this network flow is over an internal AWS network managed by Eightwire. If an attacker was able to obtain access to this network to intercept traffic (difficult, if not impossible), they would likely have obtained access to other parts of the environment, and other methods of attack would be easier.	Partially Effective	Resolve finding A10 from the AWS configuration review and enforce transport layer encryption for all AWS S3 storage buckets. Consider a future enhancement to encrypt between the load balancers and the container images, for all services. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023
C22.	Encryption of Data at Rest	Customer data is only stored in the RDS SQL databases for Conductor and Blob, and this is encrypted. There are AWS S3 storage buckets that are not encrypted. These are not used to store customer / sensitive data. The Agent configuration is encrypted once the agent update process has completed. In testing by ZX Security, it is not encrypted after the initial install.	Partially Effective	Encrypt all AWS S3 storage buckets (for defences in depth). Ensure the agent configuration is encrypted during the initial install process. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023
C23.	Cryptographic Key Management	See Control Assessment Report for more details.	Effective	
C24.	Physical Security Perimeter		Not Used	
C25.	Equipment Siting and Environmental Security		Not Used	
C26.	Standard Operating Procedures	See Control Assessment Report for more details.	Effective	
C27.	Automation and Orchestration		Not Used	
C28.	Change Management	See Control Assessment Report for more details.	Effective	

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
C29.	Performance and Capacity Management	See Control Assessment Report for more details.	Effective	
C30.	Separation of Pre-Production Environments		Not Used	
C31.	Malware Protection	See Control Assessment Report for more details.	Effective	
C32.	Backup and Restore	See Control Assessment Report for more details.	Effective	
C33.	Event Logging, Alerting and Auditing	See Control Assessment Report for more details.	Effective	
C34.	Security Information and Event Management (SIEM)		Not Used	
C35.	Clock Synchronisation	See Control Assessment Report for more details.	Effective	
C36.	Configuration Management		Not Used	
C37.	Release Management	See Control Assessment Report for more details.	Effective	
C38.	Patch and Vulnerability Management	See Control Assessment Report for more details.	Effective	
C39.	Hardening of Systems, Network Devices and Applications	See Control Assessment Report for more details.	Effective	
C40.	Security of Network Services	See Control Assessment Report for more details.	Effective	
C41.	Denial of Service (DoS) Protection	See Control Assessment Report for more details.	Effective	
C42.	Intrusion Detection and Prevention		Not Used	
C43.	Tenant Segregation		Not Used	
C44.	Firewalls	See Control Assessment Report for more details.	Effective	
C45.	Web Application Firewall	See Control Assessment Report for more details.	Effective	
C46.	Message Integrity	See Control Assessment Report for more details.	Effective	
C47.	Non-Disclosure and Confidentiality Agreements		Not Used	
C48.	Secure Application Development	See Control Assessment Report for more details.	Effective	
C49.	Due Diligence	See Control Assessment Report for more details.	Effective	

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
C50.	Contractual Agreements and SLA	Although not documented as a contractual requirement, Eightwire have already started providing monthly reports that include reporting on the implementation of the key security controls by subscribers. The document "Appendix 6 to Schedule 6, of the Ministry of Social Development and Eightwire Limited Master Services Agreement" does not include any requirements regarding: • Logging and auditing requirements, including retention requirements. • Patching requirements. • Platform security testing (such as penetration testing) requirements. • Reporting requirements for key security controls Response and resolution times are defined.	Partially Effective	It is recommended that Agencies identify their security requirements and include these in any contracts with Eightwire. Eightwire can be proactive and include many of these in the contract as standard, showing how they securely manage and maintain the platform, such as: • Logging and auditing, including retention. • Patching process and timeframes. • Platform security testing (such as penetration testing) schedule. • Configuration review schedule. • Customer right to audit. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023
C51.	Exit Strategy		Not Assessed (Not Key Control)	
C52.	ICT Supply Chain Management		Not Used	
C53.	Vendor Management		Not Used	
C54.	Information Security Incident Management	See Control Assessment Report for more details.	Effective	
C55.	Information Security Continuity		Not Used	
C56.	Business Continuity Plan		Not Assessed (Agency Control)	
C57.	Disaster Recovery Plan	See Control Assessment Report for more details.	Effective	
C58.	Fault Tolerance		Effective	
C59.	Independent Review of Information Security	See Control Assessment Report for more details.	Effective	
C60.	Architecture and Design Review		Not Used	
C61.	Defence in Depth		Not Used	
C62.	Security Tests and Controls Audit		Not Assessed (Agency Control)	

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
C63.	Service Roadmap		Not Used	
C64.	ITIL Incident Management		Not Used	
C65.	Federation Configuration		Not Used	
C66.	Cloud platform -Access Key Management Plan		Not Used	
C67.	Penetration testing and vulnerability scanning	See Control Assessment Report for more details.	Effective	
SC01.	Email Protection Agency – Filtering to protect against phishing attempts Eightwire – SPF, DKIM, DMARC	See Control Assessment Report for more details.	Effective	
SC02.	Non-persistent data transfer Ensuring that the DX does not retain data after it is processed.	See Control Assessment Report for more details.	Effective	
SC03.	Acceptable Data Assurance Ensuring that only data covered by an approved MoU is shared via the DX.	See Control Assessment Report for more details	Effective	
SC04.	Privacy Impact Assessment Conduct a PIA.	See Control Assessment Report for more details	Effective	
SC05.	Destination Update Options Receivers of information can control how data is recived (i.e. overwrite, append, merge or create new).	See Control Assessment Report for more details	Not Effective	
SC06.	Agency Data Restricted to NZ Restrict data processing to onshore.	See Control Assessment Report for more details	Ineffective / Not Present	**Remediation agreed with Responsible Manager** Due to the migration approach this needs to be verified as operational by Eightwire during the cutover to AWS. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** During cutover.
SC07.	Data Level Transfer Only Ensuring that the DX transfers the actual data rather than transferring entire files (unless file transfer is enabled), to protect against malicious code embedded in files.	See Control Assessment Report for more details	Effective	

#	Control Description	Control Implementation	Control Effectiveness	Agreed Outcome
SC08.	Service Reporting Eightwire to provide monthly reports on how key security control objectives are being met.	See Control Assessment Report for more details	Effective	
SC09.	Memorandum of Understanding MOUs are agreed between all parties, and the DX can tag transfers with the relevant MOU detail.	See Control Assessment Report for more details	Effective	
SC10.	Agent Authentication	See Control Assessment Report for more details	Effective	
SC11	Sharing One-time Code	See Control Assessment Report for more details	Effective	
SC12	Mask Data Store Credentials	See Control Assessment Report for more details	Effective	
SC13	Timeout Password Reset Links	Password reset emails do not time out.	Ineffective / Not Present	**Remediation agreed with Responsible Manager** Eightwire to configure the password reset links to timeout after 60 minutes. **Responsible Manager:** Jason Gleason, CEO Eightwire **Agreed Implementation Date:** 28/02/2023