Description of data processing – SD-WAN Cisco Catalyst

Categories of Data Subjects

(i) Users authorised by you to use the Service ("**Authorised Users**") and any employees, agents, advisors, and other authorised representatives of Authorised Users; and/or

(ii) The devices of persons connecting to your network or systems, or details about persons attempting to connect or gain access to your network ("**Network Users**").

Categories of Personal Data

Transfer (a): **User account and log details**: Details required to create Authorised Users' accounts, such as first / last name, email address, role/ job title, IP address, and company locations;

Transfer (b): **Portal activity**: Generated through the Authorised User's activity on the platform, such as details of changes made by individual users, detail of the change and the relevant date, web browser local Storage; and/or,

Transfer (c): **Network device information**: Information about devices connected to the network, which may indirectly identify individuals. This includes IP address and MAC address of end user desktops and devices, unique identifiers, device type, carrier, operating system, model, system, geo-location information (reverse IP look-up, GPS coordinates, Wi-Fi, cell ID) of end-user desktops and devices.

Telstra does not collect or transfer any special categories of Personal Data as part of this service. Additionally, Customer has the option of disabling the transmission of some categories of system information, such as SD-WAN telemetry data and Cisco Catalyst SD-WAN analytics.

The parties acknowledge that the data processed for this Service is limited to data within the portal environment and Telstra does not Process any Personal Data comprised in the contents of communications data sent and received over Customer's network and devices, either as a Controller or a Processor. Customer must ensure that all its network traffic in relation to this Service is encrypted and Customer shall indemnify Telstra in respect of any liability arising from its failure to do so (which for the avoidance of doubt includes any liability to implement measures to comply with applicable data protection laws, take steps to inform data subjects or relevant authorities of any Personal Data processing performed by Telstra on Customer's behalf and for any fines, penalties or costs of any kind (including remediation and audit costs) arising out of, or in connection with the processing of Personal Data on Customer's behalf in relation to this Service).

Commented [MR11]: Product: Please confirm if all type of authentications are being offered. See note below from the Privacy Data Sheet:
"Note: For authentication, customer may elect to use local authentication, Cisco CCO, Okta, or other third-party identity providers (IDP), such as Radius or TACACS.

Commented [DH2R1]: For Telstra, authentication is done via a IDP. For Telstra staff uses Microsoft EntraID

Commented [DH3R1]: Reviewed with Adnan.

Commented [GL4R1]: I have confirmed with Irene Ho of IP Eng that Int'l adopted the same approach as domestic fo

Commented [MS5R1]: Thanks Gary and Dan! Since our audience is our customers, does this mean we just need to

Commented [DH6R1]: Yes

Commented [MS7R1]: Updated

Commented [MR18]: Product, Regarding the End User Device IP address collection. The privacy sheet refers to "

Commented [DH9R8]: Reviewed with Adnan- we don't believe the info in the devices contains PII data to identify

Commented [GL10R8]: Agreed with Dan and Adnan. Same principle applies for Int'l customers.

Commented [MS11R8]: Are you able to send some screenshots of network device information that's available

Commented [AT12R8]:

Commented [MS13R8]: Resolved per email chain

Commented [MR114]: Product: Please confirm that Cisco ThousandEyes WAN Insight and Cisco Success

Commented [DH15R14]: This is not part of the standard offering. We are aware of Thousand Eyes but don't famili

Commented [GL16R14]: Thousand Eyes is not part of GMNS Cisco SD-WAN offer. Such request will have to g

Commented [MR117]: Product: Please confirm if these are correct. There doesn't seem to be much detail on the

Commented [DH18R17]: This is okay- reviewed with Adnan.

Commented [GL19R17]: This is correct.

Commented [MR120]: Product: Is there any action required re the info below from the Privacy Sheet?

Commented [DH21R20]: No action required.

Commented [DH22R20]: Reviewed with Adnan.

Nature of the processing, frequency of the transfer, and data retention periods

Transfer	Nature of processing	Frequency	Data Retention
Transfer (a): User account and log details, Transfer (b): Portal activity; Transfer (c): Network device information	Storage and hosting by the Subprocessor listed in this document. Access by this Subprocessor and Telstra personnel and/or affiliates for account support and customization.	Continuous storage and hosting and remote access on an as needed basis	Personal data is retained while your service is active, and any data retained following this period is anyonmized.

Technical and organisational measures to ensure the security of Personal Data

Telstra protects all third country transfers of Personal Data, undertaken by Telstra personnel or affiliates as detailed in this document, in accordance with our suite of information security standards. These standards define a number of baseline controls, which are implemented at appropriate risk based levels to protect the confidentiality, integrity and availability of both Telstra core and customer specific data. The controls and practices detailed in the standards align to industry practices and standards, such as ISO/IEC 27001:2013, ISO 31000:2009, NIST and PCI DSS. Telstra can provide details of our current certifications upon request from customers.

Commented [DH23]: Where is this sourced from?

Commented [MS24R23]: This is standard language approved by the security team.

Telstra conducts periodic reviews of the information security standards, and may therefore amend the below baseline controls from time to time to align with industry security standards and the evolving risk landscape:

Commented [GL25]: Are these standards generic and not specific to Cisco SD-WAN?

Commented [MS26R25]: This is standard language approved by the security team.

Standard	Practices
Access Control	**User access responsibilities**: Telstra staff are only able to use approved, authenticated, and encrypted remote access communication methods to log into Telstra's network and access any Personal Data. **Identification**: Telstra users are granted a unique ID before being granted access to any systems containing Personal Data, so that access is logged and monitored. **Role assignment and role based access control**: Telstra implements and maintains system and application access profiles based on the principle of least privilege, which means that staff are only provided with the minimum access to Personal Data required to perform their role. This includes record-keeping of authorised system users with access to Personal Data and governance procedures around these records, such as the annual revalidation or certification of user access requirements. **Passwords and authentication mechanisms**: Telstra uses authentication methods that are capableof validating passwords in-line

	with Telstra's standards for password strength and complexity. Passwords are also encrypted at rest.
Application security	**Developer training and awareness**: Software developers are trained on foundational concepts for building secure software including secure design, threat modelling, secure coding, security testing, and best practices surrounding privacy. **Application design**: Telstra requires that applications are signed to disabling or restrict access to system services, applying the principle of least privilege, and employing layered defences wherever possible. This includes a requirement that all third-party software is securely configured to recommended vendor security configuration, or Telstra standards, and applying strict controls around access to repositories containing Telstra source code.
Change and Configuration Management	**Process and procedures**: Telstra does not permit Personal Data to be used for development purposes – non-production and production environment must be separated and, at a minimum, enforce logical isolation. **System and server configuration**: Telstra maintains security configuration baselines consistent with industry accepted hardening standards, which address known security vulnerabilities, and communicates these to relevant personnel. Servers are specifically configured to prevent Personal Data from being exported to unauthorised users.
Cryptography	**Cryptographic algorithms**: Only Telstra approved algorithms may be used, and Telstra requires that system configuration support is removed for all weak, non-approved algorithms. Access to encryption keys is recorded and audited at least annually.
Data Protection	**Information classification**: Personal Data is classified as such to meet applicable requirements under data protection laws. This enables Telstra to remove Personal Data from datasets, if not required to provide the agreed service or meet regulatory requirements, and to remove or protect direct identifiers of Personal Data in datasets, using approved algorithms or software. **Information handling:** Telstra staff must protect Personal Data by using approved encryption methods when it is been stored and transmitted, only using authorised file sharing services, and locking devices when not in use. At an application level, Telstra solutions must meet data segregation requirements, so that each customer's data is logically separated from other customers' data and users can only see customer data that they require for their role
Incident Management	**Incident response plan:** Telstra maintains and tests an incident response plan, which is supported by the designation of personnel who are available on a 24/7 basis to respond to alerts, along with training to all staff with security breach response responsibilities.
Logging and monitoring	**Audit log content and trails:** Telstra implements audit trails that link system component access to individual user accounts to reconstruct

	access to Personal Data. Logs for systems that store, process, or transmit Personal Data are continually reviewed
Network Security	**Network management:** Telstra operates procedures for monitoring access to network resources and sensitive data environments, and uses intrusion detection / prevention techniques on traffic entering its internal network.
Physical Security	**Facility controls:** Telstra limits and monitors physical access to systems containing Personal Data by requiring that access is authorised and based on individual job functions, any third party access is vetted and approved, and access is revoked immediately upon termination. **Data centre physical access:** Telstra restricts entry into server rooms and protects against unauthorised access by logging entry and exit, requiring a special code or key for entry, and configuring access controls to continue preventing unauthorised entry if power is lost
Staff security	**General security culture and conduct:** Telstra maintains a formal security awareness program so that staff are aware of their security responsibilities. This includes providing an annual security module to all staff and additional role-based training for relevant personnel. **Background checks:** Telstra staff undergo relevant and appropriate background checks.
Supplier Management	**Due diligence:** Telstra requires that a partner security assessment is undertaken for suppliers that have the potential to access Personal Data. **Contracts:** In addition to clauses required under data protection laws, Telstra incorporates standard data security clauses into contracts for suppliers that will access, transmit, use, or store Personal Data. **Security:** Suppliers must agree to comply with Telstra security standards and any additional Telstra requirements for the secure access, exchange, and lifecycle management of Telstra information, including Personal Data; data loss prevention; and business continuity and disaster recovery.
Vulnerability management	**Vulnerability protection**: Telstra deploys penetration testing, vulnerability assessments, and periodic evaluations of malware threats to systems. **Patch management**: Telstra requires that system components and software are patched and protected from known vulnerabilities, and controls are in place to verify the integrity of patches prior to deployment.

Telstra has implemented technical and organisational measures and processes to comply with data subject rights as further detailed in Telstra's privacy statement, available at Tel.st/privacy-policy.

In addition to the supplier management controls detailed above, the following technical and organisational measures are implemented to ensure that the Subprocessor, as detailed in this document, is able to provide assistance in meeting obligations under relevant Applicable Data Protection Laws. These include:

Commented [RB27]: For SDWAN no anti malware

Commented [DH28]: This might be done by both Cisco and Telstra, depending on the item

Commented [MS29R28]: Agree - this is standard prescribed language. We try to callout the responsible party in the bullets.

Commented [MS30R28]: Tweaked the language to stay silent on which entity is implementing the measure

Commented [DH31]: What is the working definition of subprocessor in this context? Is it the entity working on behalf of Telstra for the solution?

Commented [MS32R31]: Any other entity that hosts, stores, or accesses personal data in the portal - see list in Annex III.

- System administrator log-in information and the end user device identifiers are both encrypted at rest with AES-256 algorithm and encrypted in transit with TLS 1.2.

Role based access is used to control access to the features or data on the portal that users can access, based on the principle of zero trust.

List of Subprocessors

Telstra has engaged the following Subprocessors:

- Cisco Systems Australia Pty Limited for Transfer (a): User account and log details; Transfer (b): Portal configuration and activity; Transfer (c): Network Device Information

These include applicable Telstra affiliates listed here, as updated from time to time.

Contact person details and address of the listed Subprocessors, are available upon request to Telstra at privacy@online.telstra.com.au.

Commented [DH33]: Agree

Commented [DH34R33]: Telstra controls system login and end user identifiers using audit logs of the Cisco Catalyst SDWAN Manager. Additionally, this data is sent to Splunk to manage

Commented [MS35R33]: Does that cover Cisco user logs too?

Commented [AT36R33]: Yes

Commented [MS37R33]: I think this might already be covered by the logging item in the table above?