Description of data processing – Managed SSE (Netskope)

Categories of Data Subjects

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

Categories of Personal Data

Transfer (a): **Information processed to setup the Netskope managed service:** As part of the professional services engagement you may provide Telstra with various pieces of contextual information about your network and your Network Users. This may include a list of user accounts, the names, work phone, email and work address, of the users associated with those accounts.

Transfer (b): **Security event information:** As part of reviewing policy violation alert logs, the Telstra Security Service Centre ("**TSSC**") may process your Network Users' username, user group name, IP addresses, device name and identifier, location information and the network activity that has triggered an alert. The identity of the Network User is associated with the alert, which may include details about websites and applications they have attempted to access, download activity, operating system details, traffic type, access method, and forensic data with masked previews of the information that violated the data loss prevention policy. This information will correlate to the security policies you have chosen to implement.

Transfer (c): **Information processed as part of add-on services:** If you choose to add-on Targeted Remote Browser Isolation, Zero Trust Secure Access, Cloud Firewall, Email DLP, Cloud Security Posture Management, SaaS Security Posture Management, or API-based File Protection, we may process additional information about Network Users as part of providing that service. This generally includes username, device name, user device OS, source/destination IP address, FQDN (domain name) and source/destination TCP/UDP port. Additional information about websites and URLs visited by Network Users is processed as part of Targeted Remote Browser Isolation. API-based File Protection also involves processing details about files and applications used by Network Users, including files shared to external sources, Network User location, and anomalies in Network User behaviour.

Depending on the data loss presentation policies set by you, or add-on services you obtain, the TSSC may have access to information about Network User activity, such as website and file logs, which could indirectly suggest sensitive information or special categories of Personal Data about a Network User. You are in full control of TSSC's access as you are required to provision TSSC's access within your identity provider, and subsequently configure and assign TSSC access to Netskope's management console. Your full control over the access and the data loss presentation policies provides you with an additional layer of protection.

Additionally, Netskope has implemented comprehensive logging and auditing technical features. All actions performed in the platform are logged, along with the username, detail of activity (excluding policy name), report name, added application and added action. TSSC does not have permissions to download data.

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

Transfer	**Nature of processing**	**Frequency**	**Data retention**
Transfer (a): Information processed to setup the Netskope Managed Service; Transfer (b) Security Event information; and Transfer (c): Information processed as part of add-on services	Storage and hosting by Subprocessor listed in this document with no ability to access the stored / hosted Personal Data, unless specifically authorised by you for troubleshooting purposes. Access and processing by Telstra affiliates and personnel listed in this document, to provide platform configuration, set security policies, provide monitoring and alert services, and, if requested by you, manage platform-related incidents.	Storage, hosting, and monitoring on a continuous basis; access on an as needed basis	Retention policies are set by you. You can at any time revoke access to Telstra affiliates and personnel.

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.

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:

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 capable to 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.
	Process and procedures: Telstra does not permit Personal Data to be used for development purposes, unless an exception has been approved

Standard	Practices
Change and Configuration Management	by Telstra's Security Team – 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	**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.

Standard	Practices
security	**Data centre physical access:** Telstra restricts entry into server rooms and protects against unathorised access by logging entry and exit, requiring a special code or key for entry, and configuring access controls to continue preventing unathorised 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, Personal Data; data loss prevention; and business continuity and disaster recovery.
Vulnerability management	**Vulnerability protection**: Telstra deploys anti-malware software, 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.

For Transfer (a): Information processed to setup the Netskope Managed Service; Transfer (b): Security Event information; and Transfer (c): Information processed as part of the add-on services:

- All personally identifiable information, including that related to card payments, is masked based on your data loss protection policies,
- Logs are encrypted in transit to the cloud storage of your choice and all data loss prevention forensic data and threat protection quarantine folders are also stored on the cloud storage of your choice;
- You can enable or disable sharing of log types in accordance with your policies,
- You have full control to create, delete and disable Telstra's access to the system, which has comprehensive logging and auditing technical measures, with all actions performed on the platform being logged.

List of Subprocessors

Telstra has engaged the following Subprocessors:

(1) Netskope Inc for Transfer (a): Information processed to setup the Netskope Managed Service; Transfer (b) Security Event information; and Transfer (c): Information processed as part of add-on services.

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.