Description of data processing – Managed Microsoft Defender Endpoint Detection and Response

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 Managed Microsoft Defender Endpoint Detection and Response 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): **Information processed as part of the Managed Microsoft Defender Endpoint Detection and Response Service:** To provide the monitoring and alert service, the Telstra Security Service Centre ("**TSSC**") may process network details, including inbound or outbound connections, source and destination IPs, ports, protocols and associated application data. The TSSC may also process endpoint devices information including device hostnames, device IP addresses, OS information and associated users, logs and telemetry data generated by endpoints, and high-level metadata related to accessed or modified files. The identity of the Network User is associated with the alert, which may include details about the account name and other contextual information such as the system generating the alert, the hostname/IP address associated with the alert, files and Endpoint devices. This information will correlate to the security policies you have chosen to implement.

Transfer (c): **Information processed as part of the add-on Telstra Purple Professional Services**: If you choose to add-on the Professional Services through the Telstra Purple Services, we may process information on all endpoint devices monitored through Microsoft Endpoint. This generally includes device identifiers, usernames, user device OS firewall rules, VPN configurations and proxy settings for Endpoint connectivity.

Depending on the security and alert 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 Managed Microsoft Defender Endpoint Detection and Response's management console. Your full control over the access and the security and alert presentation policies provides you with an additional layer of protection.

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 Managed Microsoft Defender Endpoint Detection and Response Service; Transfer (b) Security Event information; and Transfer (c): Information processed as part of the add-on Telstra Purple Professional 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, manage security policies, provide monitoring and alert services for threats, and, if requested by you, manage platform-	Storage, hosting, and monitoring on a continuous basis; access on an as needed basis	Retention policies 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	**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, unless an exception has been approved 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
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 implements audit trails that link system component 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 unathorised access by logging entry and exit, requiring a special code or key for entry, and configuring access controls to continue.
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.

You have control over the level of access granted to Telstra staff, which may be based on Telstra's recommendations to effectively service your needs. This access may allow Telstra staff to download logs. However, you retain the right to terminate this access at your discretion. In addition, the following technical and organisational measures apply:

- Data and logs is encrypted in transit and at rest.
- Role-based access control is implemented to ensure that only authorized personnel can access Personal Data.

- Device control capabilities and inventory management allows you to control your device inventory in accordance with your policies and procedures.
- The Subprocesser is compliant with SOC 2 Type II and the service is hosted in data centres certified as SOC 2 Type II.
- Logs stored in the Subprocessers' cloud storage are encrypted both in transit and at rest to the cloud storage of your choice and threat protection quarantine folders are also stored on the cloud storage of your choice.

List of Subprocessors

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.

The Customer acknowledges that where we or our Affiliates access Customer's Microsoft Defender Endpoint Detection and Response environment in relation to the provision of this service, we and/or our Affiliates do so acting on the Customer's behalf, using the licence that Customer has directly or indirectly procured from Microsoft, and that it is Customer's obligation to assess and determine whether entering into a data protection agreement with Microsoft is required.