Description of data processing – Managed Cloud Services

Categories of Data Subjects

The accounts 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): Active Directory Data: If requested by you as part of your IaaS / Private Cloud Service, your Hybrid Cloud service, your Public Cloud service, your DRaaS service, your BaaS service, and/or your VDI service ("**Managed Services**"), Telstra may provide managed Microsoft Active Directory or Microsoft Entra ID as a service for you. This may involve your Network Users' full name, display name, office address, work contact details, job title, and reporting lines.

Transfer (b): File Data: As part of providing Managed Services, Telstra may have visibility of file and folder names, which, depending on the naming conventions determined by you, may contain Personal Data. If requested by you, File Data may be copied from their primary location to a secondary location for backup, archive, and disaster recovery purposes.

Telstra does not collect or transfer any special categories of Personal Data as part of this service.

While some Managed Cloud Services involve Telstra managing compute, network, storage infrastructure, up to and including managing operating system, Telstra does not perform any operations on Personal Data contained within these systems, either as a Controller or a Processor, aside from the activities listed above.

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

Transfer	**Nature of processing**	**Frequency**	**Data retention**
Transfer (a): Active Directory Data	Access and Processing only upon request by Customer to grant Network Users' with access, for example, if their accounts become locked.	Access and Processing on an ad hoc basis, as requested by Customer.	Access revoked upon termination of the services. In the event that hardware containing operating system data remains in Telstra's property after the termination date, this hardware

	If requested by Customer, Telstra may Process Active Directory Data to replicate this information in the Customer's disaster recovery environment.		is deleted, reformatted, and wiped.
Transfer (b): File Data	Creation, modification or auditing of backup schedules and location upon request of customer. Visibility of file and folder names as part of routine assurance tasks.	Access and Processing on an ad hoc basis, as requested by Customer.	In the event that hardware containing operating system data remains in Telstra's property after the termination date, this hardware is deleted, reformatted, and wiped.

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, 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 Network User Personal Data. **Identification:** Telstra users are granted a unique ID before being granted access to any systems containing User 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

Standard	Practices
	the minimum access to User Personal Data required to perform their role. This includes record-keeping of authorised system users with access to User 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.
Change and Configuration Management	**Process and procedures:** Telstra does not permit User 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 all known security vulnerabilities, and communicates these to relevant personnel. Servers are specifically configured to prevent User 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:** User Personal Data is classified as such to meet applicable requirements under data protection laws. This enables Telstra to remove User 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 User 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

Standard	Practices
	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 User Personal Data. Logs for systems that store, process, or transmit User 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 User 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 User 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 User 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 User 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.

Standard	Practices
	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, Telstra also employs specific technical and organisational measures to ensure Subprocessors are able to provide assistance in meeting obligations under relevant data protection laws. These include:

Access by Sub-processors involved in Transfer (a): Active Directory Data, and Transfer (b): File Data, is either controlled by Telstra, as the Sub-processor's processing is executed within Telstra's management platform, or controlled by the Customer itself, as the Customer is the party defining (i) the scope of any back-ups, (ii) retention requirements, and (iii) storage policies for the Sub-processor's access (which is only remote).

List of Subprocessors

Telstra has engaged the following Subprocessors:

- Accenture Australia Pty Ltd for Transfer (a): Active Directory Data and Transfer (b): File Data.
- Databarracks Limited for Transfer (a): Active Directory Data and Transfer (b): File Data.

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

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

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