PUBLIC

Information Security Policy

Version 14 – March 2022

data zoo

The information in this document is published, "as is". Data Zoo makes no representations or warranties with respect to the information provided in this document.

Data Zoo is of the opinion that the information in this document is accurate as at the date of this publication. Data Zoo has made every effort to ensure the accuracy of the information contained in this document, but it is the responsibility of Data Zoo's clients to make an independent assessment as to the correctness of the information provided.

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this document is uncontrolled and cannot be relied upon.

1. Introduction

1.1 Terms and Definitions

"we", "us" and "our" refer to Data Zoo. "staff" and "users" means all of those who work under our control, including employees, contractors, interns etc.

1.2 Basic Information Security Terminology

Confidentiality – characteristic of the information by which it is available only to authorised persons or systems.
Integrity – characteristic of the information by which it is changed only by authorised persons or systems in an allowed way.
Availability – characteristic of the information by which it can be accessed by authorised persons when it is needed.
Information Security – preservation of confidentiality, integrity and availability of information.
Information Security Management System (ISMS) – part of overall management processes that take care of planning, implementing, maintaining, reviewing, and improving the information security.

1.3 Purpose and Scope

The aim of this top-level policy is to define the purpose, direction, principles and basic rules for information security management. The purpose of this document is to succinctly communicate our security policies.

1.4 Users and Responsibilities

Users of this document are all our staff, as well as relevant external parties. Further details and explanations can be provided by the Data Zoo Compliance Team on request. The ISMS Manager is responsible for all aspects of the implementation and management of these arrangements, unless noted otherwise. Managers and supervisors are responsible for the implementation of these arrangements within the scope of their responsibilities and must ensure that all staff under their control understand and undertake their responsibilities accordingly.

2. Compliance and Assurance

2.1 Compliance Framework

We have developed a compliance framework that enables the organisation to effectively identify and manage information security, privacy, and business risks. We ensure the security and confidentiality of the Source Data that is supplied under the agreements from customers for the verification of their individuals. Data Zoo is ISO 27001:2013 certified for Australian operations; has been issued SOC 2 Type 1, Type 2, SOC 3 and ASAE 3150 reports; adheres to relevant GDPR and CCPA controls; and is working towards ISO 27701:2019. Data Zoo GDPR Compliance can be viewed at: https://www.datazoo.com/compliance.

2.2 ISO 27001:2013 Certification

We have designed, developed, and implemented comprehensive information security controls in our ISMS to establish, monitor and continually improve our safeguards for the confidentiality, integrity and availability of all physical and electronic information assets. Our ISMS is aligned to the ISO 27001:2013 standard, which has been certified by a JAS-ANZ accredited body for the organization's Australian operations. Certification can be viewed at: https://www.datazoo.com/compliance

2.3 SOC 2 Type 1 & 2 & SOC 3 Reports

Data Zoo has completed SOC 2 Type 1 & Type 2 audits for relevant Security Trust Service Criteria (TSP), with supporting SOC 2 Type 1, Type 2, and SOC 3 reports issued to the organisation. We can provide a copy of the respective reports upon request.

2.4 Australian Open Banking (CDR) Accreditation & ASAE3150 Reports

We have successfully completed ASAE3150 audits and is now Accreditated Data Recipient (ADR) as per Australian Consumer Data Rights. We can provide a copy of the respective report upon request.

3. Risk and Information Security

3.1 Risk Assessment

We have adopted a straightforward risk assessment methodology; undertaking an information security risk review throughout the organisation that takes account of the established criteria, at periods not exceeding 12 months, or when significant changes are proposed or occur. The review is undertaken under the direction of the ISMS Manager and draws on both internal, and where required, external expertise. Data Zoo analyses and evaluates identified risks to gauge their severity, probability, and controllability and determines a relative Risk Index score. The respective Risk Index scores are evaluated against approved criteria (for accepting risks and identifying the acceptable levels of risk) to identify and prioritise risks requiring treatment. Where a risk is deemed to require treatment, or there is a legal requirement to do so, the ISMS Manager consults with the risk owner and the owner of the information assets, as well as with those with expert knowledge if necessary, to agree on appropriate methods to eliminate or lower the risk to an acceptable level. Based on the outcome of this consultation, a Risk Treatment Plan is prepared and a Corrective Action Plan is devised. The ISMS Manager and Compliance Team maintain appropriate records of the information security risk assessment process and its outcomes. Our risk assessment practices are continually reviewed internally to ensure a pragmatic business-led approach is adopted, best practice is maintained, and continuous improvement is achieved.

3.2 Ongoing Compliance And Assurance

Data Zoo conducts internal audits on its ISMS every 6 months. An audit plan is prepared by the internal auditor, which details the audit scope, audit objectives, and audit criteria to be covered in the internal audit. The internal auditor works with the appropriate managers and employees to review the respective processes in the context of the expected information security and privacy controls, facilitating technical compliance tests where necessary to verify IT Systems are configured in accordance with policies, standards and guidelines. Where any non-compliance is identified, the responsible manager, in consultation with the ISMS Manager, determines the root cause of the non-compliance, evaluates the need for actions to ensure that non-compliance does not reoccur, devises a corrective action plan, and reviews the corrective action taken to ensure outcomes are as expected.

We conduct quarterly vulnerability and penetration testing on all of our systems to ensure technical resilience. In line with the ISO 27001:2013 standard, we are subject to annual external surveillance audits, with a recertification audit every 3 years. We are subject to annual SOC 2 Type 2 audits of implemented Trust Services Criteria (TSP) as required by the framework. In addition, we are subject to demonstrate adherence to CDR rules on an annual basis.

3.3 Vulnerability Assessment and Penetration Testing

Penetration tests or vulnerability assessments used at Data Zoo follow a formal methodology as per our Vulnerability Management Procedure; they are carefully planned, exercised with due caution, are designed to be repeatable. Penetration and vulnerability testing is completed every quarter by industry recognised professionals, with any outcomes/recommendations actioned immediately. In addition, host scanning is conducted every three months. We can provide a copy of the latest Vulnerability & Penetration Assessment Summary upon request.

3.4 Roles and Responsibilities

We recognise the importance of designating competent and appropriate resourcing to meet our compliance commitments and ensure information security and privacy. We have appropriately assigned and communicated all roles and responsibilities of our compliance framework to fit and proper staff. These roles and responsibilities are documented in our Roles and Responsibilities Register.

4. Information Handling

4.1 Personally Identifiable Information (PII) Protection

We consider Personally Identifiable Information (PII) to be treated with utmost degree of sensitivity, and deserving of the highest information classification rating for information assets as outlined in our Information Classification and Handling Policy. Confidentiality of PII stored for transactional purposes is achieved via hashing in accordance with our Information Classification and Handling Policy and our Cryptographic Controls Policy. Different hashing schemes have been developed for individual PII fields based on their classification level. We comply with the Australian Privacy Act (1988) and adopt GDPR best practices for the management of PII. We take a transparent approach to the handling of PII in line with CCPA obligations. We do not store any PII beyond the duration of the transaction nor sell/transfer it to any third party for primary or secondary, unrelated reasons without the informed consent of the identity owner (captured and relayed via our clients). We ensure that all clients and related parties sign suitable contracts for access to the data. These contracts will highlight the penalties of any misuse by the company and that it is the responsibility of the company to ensure that their internal process implements the terms and use of the data.

4.2 Data Destruction

We have a dedicated Data Disposal Policy in place which provides techniques, guidance, and definitions to data destruction practices and considerations. All customer's client data is disposed of when it is no longer necessary for business use. Unless advised, customer information is stored for a maximum of 24 hours to generate transaction reports. Customers can request to deactivate the retention period. Data Zoo provides electronic verifications via API, Batch, or the IDU Web Application.

API – all transaction logs and search summary reports are one-way hashed to de-identify PII immediately prior to secure storage. The search summary reports remain available for 24 hours after the search to enable customer access for retrieval (if required for reporting purposes).
Batch – all transaction logs and search summary reports are one-way hashed to de-identify PII prior to secure storage. Further, the result customer files are deleted from the SFTP service 24 hours after delivery.
Web – all transaction logs are one-way hashed to de-identify PII immediately prior to secure storage. The search summary reports remain available for 24 hours after the search to enable customer access for retrieval (if required for reporting purposes).

All physical devices and media that are retired from the organisation's use are securely removed, destroyed, and overwritten in line with our Data Disposal Policy.

4.3 Data & Service Integrity

Our identity verification solution is underpinned by a thorough, legitimate, and workable regulatory environment and powerful policies advocating trust in the digital identity verification service; ensuring data protection, privacy, and ensuring accountability. We ensure the integrity of all services and data sources through a rigorous quality assurance process, consisting of both manual and automated testing processes. The automatic monitoring is done via FreshPing which allows us to maintain an active system monitoring application that routinely and in real-time verifies that our services are online and responsive. Customers are able to view this service on our Support Portal: https://datazoo.freshdesk.com/support/home. The manual testing is done by running checks via our system at regular intervals, against selected data sources to verify the actual service I/O and to ensure they are working as expected. This is achieved through Postman Monitoring. This testing regime reports on expected and actual results with exceptions promptly investigated by our support staff. The aim of this testing is to ensure response structures and data formats remain consistent.

4.4 Data Life Cycle Management

We consider privacy in all stages of the data lifecycle. It ensures that data acquisition processes are adequate to capture all data needed to perform the transaction. We does not store any PII beyond the duration of the transaction. Any data (i.e. transaction logs) that is to be stored is then stored and secured in an optimal manner to minimise storage requirements and to be accessed in the fastest possible manner. Once the data is securely stored and is available to be accessed, it is then discovered and classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification (against one of the four levels of classification outlined in our Information Classification and Handling Policy). After data has been used and is no longer needed, it is destroyed in accordance with our Data Disposal Policy. Please refer to the table below for a summary of Data Life Cycle stages.

Table 4.4.1 – Data Life Cycle Management

Stage	Protection Procedure
Collection/Transmission	Data is transferred via SOAP and/or RESTful web service calls via HTTPS.
Use	All sensitive data is hashed after the completion of the transaction so that it can never be reidentified.
Retention	We do not retain any kind of identifiable client PII beyond the duration of the transaction, as per our information classification policy. PII is retained for 24 hours to generate transaction reports only and de-identified after 24 hours.
Destruction	Data is destroyed when no longer needed.

4.5 Asset Management

We ensure that all critical assets associated with information and information processing facilities are identified and listed in the Information Asset Inventory, which is maintained by the Compliance Team. Each listed asset is allocated an "owner" and assigned an information classification in line with the scheme defined in our Information Classification and Handling Policy. We have defined and implemented an Acceptable Use Policy, that details the requirements for acceptable use of assets, which all staff are informed of and required to meet. We ensure the appropriate handling of information assets per their information classification.

5. Access Controls

5.1 Access Control Policies

We evaluate risks relating to access controls and implement supporting controls accordingly in our Access Control Policy. Access is granted using the principle of 'Least Privilege', whereby every program and user of the system should operate using the least set of privileges necessary to complete the job. Formal and proven procedures are used for access provisioning and de-provisioning, and periodic reviews of access (Periodic Access Review Plan) are undertaken to ensure integrity.

5.2 System Access Control

Access to our services is granted through the individual allocation of user rights and requires authentication by username and password. We have implemented a formal Password Policy, which specifies both the technical requirements for passwords as well as the expected procedures and practices related to password management by staff. We manage all official passwords via LastPass, which is enforced, monitored and managed under the Data Zoo Mobile Device Management program (see below). We require customers to supply their IP addresses for security and use of its services via IP Whitelisting. Our system will automatically IP block a Customer account if more than 10 sequential incorrect credentials are provided within 24 hours. Access to configuration management is only by our Support staff and is reinforced with multi-factor authentication processes. All changes (data source access, configurations etc) to accounts are logged and monitored regularly.

6. Information Security Incident Management

We have implemented a formal Incident Management Policy to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. All staff and suppliers are required to promptly report any suspected information security events to Incident Management Team (IMT) or Senior Executive Management Team SEMT) depending on the severity of the incident. The responsible team then works together to complete an Incident Report Form. We require all malfunctions and anomalous system events involving classified information to be reported as an information security event, as they may be an indicator of a security attack or actual security breach. When an information security event is reported, the IMT or SEMT assesses the event to see if it should be classified as an incident and, where necessary, takes immediate remedial action to alleviate the threat. The details of the incident, remedial action taken, and outcome are recorded in a formal register for improvement and audit purposes. Figure 6.1 summarises the incident management workflow and response procedure:

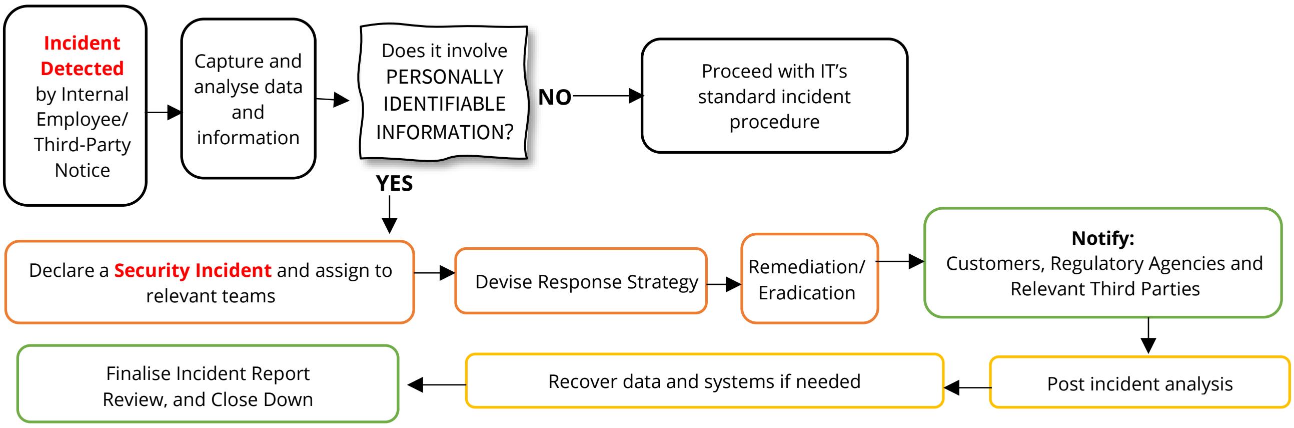
Incident Detected by Internal Employee/ Third-Party Notice
Capture and analyse data and information
Does it involve PERSONALLY IDENTIFIABLE INFORMATION?
NO
Proceed with IT's standard incident procedure
YES
Declare a Security Incident and assign to relevant teams
Devise Response Strategy
Remediation/ Eradication
Notify: Customers, Regulatory Agencies and Relevant Third Parties
Post incident analysis
Recover data and systems if needed
Finalise Incident Report Review, and Close Down

Figure 6.1 Incident Management Workflow

Change Management

6.1 Change Management Procedures

We utilise formal procedures to address risks related to changes in systems and business circumstances. All changes are subject to the Change Management Policy, which requires changes to be assessed in line with the operational risk profile of the change to ensure all procedures have been followed. All changes require an appropriate level of testing to be undertaken which provides a high level of confidence that the change will be successful and will not negatively impact production functionality. Any changes deemed to present an unacceptable level of risk are to be denied. All changes must be logged appropriately alongside any supporting documentation and approvals for audit purposes.

6.2 Security in Change Management

We consider the security requirements of each request for change from a risk perspective, considering the risk, likelihood, required mitigation, and ultimately the risk severity. An information security testing plan was developed and followed for all significant changes in our information systems, applications, or network infrastructure, prior to releasing the change to the production environment. The plan must include the testing of the design and operation of the security controls determined during the request for change security assessment. All information security testing activities are performed in a non-production environment (e.g. dedicated test environment) and must be signed-off by our Head of Solutions before the change is rolled out to the production environment.

6.3 System Security

Our servers are protected by Next-Gen Firewall appliances with intrusion prevention systems (IPS) to identify and block threats in real-time. The cloud service provider is responsible for controlling access, logging and monitoring of the systems and infrastructure. In addition to this, we uses Cloudflare's globally managed DNS service as a gateway to provide an additional layer of security as well as service continuity through load balancing and failover services. The architecture of the application is n-tier. Client data is stored inside of a trust zone, which is behind a DMZ. (i.e. the product is supported by best practice application architecture). Access to the application is via username and password that has industry-standard strength requirements.

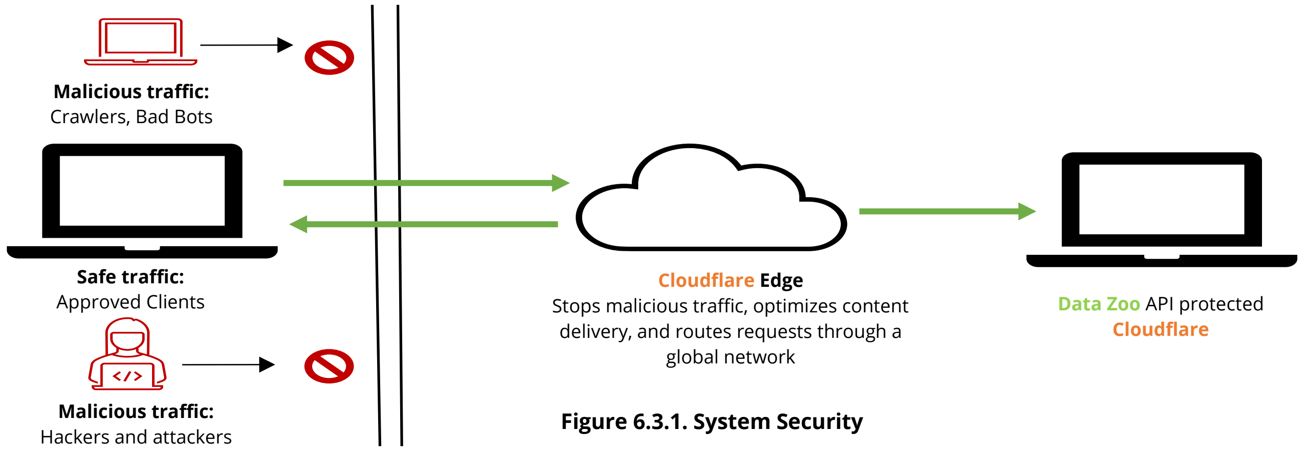

Figure 6.3.1. System Security

6.4 Backup and Recovery

Backup copies of information, software and system images are taken and tested regularly in accordance with a formal Backup and Restore Policy. We ensure that the extent, frequency, and retention period of backups reflect business requirements, security requirements, the criticality of the information to continued operations, and legal or audit requirements. Where backup arrangements are automated, such automated solutions must be sufficiently tested prior to implementation and at regular intervals thereafter. Data restores are only undertaken by competent, authorised staff.

6.5 Logging & Monitoring

Event logs recording user activities, exceptions, faults and information security events are produced, stored and regularly reviewed. Logging facilities and log information are protected against tampering and unauthorized access. System administrator and system operator activities are logged, and the logs are protected and regularly reviewed in line with formal access review procedures. The clocks of all relevant information processing systems are synchronised to a single reference time source. All PII stored in logs is hashed after completion of transaction so it cannot be reidentified in any way, shape or form. For API and web users, we log and monitor IP addresses for each server access. We capture IP ranges for clients at the time of signup and validate the IP's accessing our servers to ensure no unexpected traffic. These IP addresses/ranges are classified as business confidential information and are never accessed for a reason other than for support processes or traceability of incidents.

6.6 Test Data Management

Test data and the testing environments are completely independent of the production environments. Our testing environment is not a sandbox environment and has been developed and designed specifically for the testing of our services. The test data is provided by a new data source and compiled by our Testing Team at the time of testing commencement. All security and permissions for testing are negotiated with our Testing team which in turn coordinates with the various teams within Data Zoo to facilitate testing.

7. Device Security

7.1 Mobile Device Management (MDM)

All our employee machines are enrolled into a centralised MDM Program (managed by a trusted and recognised third-party provider) to ensure they adhere to all required technical compliance controls in accordance with our Mobile Device Management Policy. Employees are restricted from installing or removing applications from their machines without appropriate IT approval and intervention, and all updates to operating systems, anti-virus, and other applications are tracked and enforced remotely. Additionally, all Data Zoo employee Mobile Phones used for work purposes must be enrolled into the MDM program, enforcing required technical controls (such as passcode complexity and automatic screen locking) and ensuring all Data Zoo information is protected within a "secure bubble" on the device. Employees are not able to transfer or copy information of any kind (text, images, screenshots, etc) outside of the Data Zoo "secure bubble" on their mobile phone into their personal applications or documents, with the MDM program supporting remote deletion of all Data Zoo information and applications from the device in any instance of compromise or non-compliance. All devices enrolled into the MDM program have encryption technically enforced.

7.2 Acceptable Use of Devices and Secure Employee Behaviour

Upon onboarding, all our employees are required to acknowledge and adhere to the Acceptable Use Policy, and Disciplinary Policy. Employees are given formal Information Security Awareness training to be made aware of their personal responsibilities in regards to Information Security and Privacy. Secure behaviour is instilled into all our staff, which includes employees being required to screen lock their devices when stepping away from them both in and out of our authorised offices or teleworking spaces. It is not permitted to leave these devices unattended in any other setting, such as a public place or vehicle, or with any unauthorised persons for safekeeping. Our employees are trained and reminded to remain vigilant at all times in order to safeguard information and data and to protect the security and integrity of our IT systems. They must report any suspicious or unknown equipment or persons near Data Zoo devices to their line manager or a membe of the management team immediately.

8. Physical Security

8.1 Physical Security and Environmental Security

Our Sydney office premises is securely guarded with 24-hour surveillance. Access to the office is restricted to only authorized people with the provision of keys. Guests need to register at the reception and are required to be escorted at all times in the offices we occupy. The shared office space goes into lockdown after 5:00 pm. "Out of office" hours access is only provided through a registered fingerprint system. Appropriate physical protection, and contingencies against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster are in place, and are periodically reviewed. Our additional office locations also have adequate physical security measures to secure access to company facilities, equipment, and resources, keeping unauthorized personnel away. As mentioned above ("7. Device Security") mobile assets such as laptop computers, are secured through enrolment and management. Our API is deployed on the Google Cloud Platform ("GCP") whose physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data centre floor features laser beam intrusion detection.

8.2 Data Centers

We store all data on a cloud-based server, utilising firewalls and advanced encryption, which is used to protect all data and our applications. Databases have built-in security that prevents unauthorised access from malicious actors. All transactions are user and IP address logged. Data Zoo cloud-based servers are globally located ensuring minimal cross border information transfer. Data is processed in the legal jurisdiction. Our servers are located in AU, NZ, Singapore, and the EU. Additional servers can be set up on demand, in any country within 3 weeks. Databases are backed up multiple times a day. There is failover capability between multiple servers within each data centre, as well as automated failover processes between data centres should an entire data centre go offline. We have processes in place to monitor and test the failover sites as required to ensure the capacity for redundancy remains in place. There are frequent synchronisation activities in place to ensure configuration and account management is identical between all servers thereby eliminating downtime in instances where traffic is re-routed between the servers and data centres. For more information on how we manage data centre security or for data centre technical specifications please contact your account representative or contact us via info@datazoo.com.

9. Network Security

Data Zoo does not have an internal network. Network security is managed and controlled by the respective building managers at each of our offices, to protect the information in systems and applications. Security mechanisms, service levels and management requirements of all network services are identified and included in-network services agreements, for both in-house and outsourced services. Groups of information services, users and information systems are segregated on networks. Onsite, our staff use protected WiFi provided by the building manager i.e., WPA2-enterprise encryption SSID. Offsite, our staff use private protected WiFi or Personal Hotspots. The IPs of all staff who have access to Data Zoo infrastructure are registered and whitelisted.

10. Business Continuity and Disaster Recovery

10.1 Business Continuity Management

Data Zoo has in place a Business Continuity and Disaster Recovery Plan (BC&D Recovery Plan) defined and documented, which explicitly states the contingency procedures required to continue, restore and recover core services and operations in the event of a disaster. We undertake regular BC&D Recovery Testing utilising tabletop and technical recovery testing to test resilience to disruptions and effectiveness to restore operations.

10.2 Pandemic Business Continuity Management (Pandemic BCP)

In response to the risks presented by COVID-19, Data Zoo has set out the framework for Business Continuity Management (BCM) with plans and procedures for the recovery of business-critical processes in the event of a Pandemic. The objective of the Pandemic BCP is to recover the critical and material processes, computer systems and communications network of Data Zoo to an acceptable level in the shortest possible time, with minimal disruption to all the departments and their services to clients, accounting for additional considerations and contingency presented by pandemics. With careful preparation, we are able to activate our Teleworking Policy and resume normal operational service with minimal disruption. A copy of the Pandemic BCP can be provided upon request.

11. Legal and Regulatory Compliance

11.1 Cross Border Transfer Of Information

Our policies are designed to ensure that all information is secure both in internal databases and when our customers are accessing it. Access to systems is monitored electronically, providing an auditable record of who, what and when data was accessed. Where applicable and required by the business process, data does not leave the country of data source processing - and only the actual verification results are returned to our systems.

11.2 Insurance

We maintain Public Liability, Product Liability, Professional Indemnity, and Cybersecurity insurance at all times. These insurance policies have been included as part of the SOC 2 audit. Data Zoo actively reviews the insurance on a needs basis or otherwise at least once a year. We expect and request a similar level of insurance coverage from our contracting counterparts.

12. Supplier Due Diligence

We have measures in place to ensure our data sources are externally verified and certified to ensure reliability, accuracy, and legality of service. All our data source suppliers (“Suppliers”) undergo robust due diligence in addition to an annual vendor risk management exercise (including a security questionaire) that we perform on them via OneTrust Vendor Risk management. Our Suppliers are expected and required to adhere generally and specifically to this policy. Specifically, they are required to implement the technical and organisational measures described in the table below to protect the Services and the Data Zoo Data in such a way as to ensure a level of security appropriate to the risk. Please note that if a Supplier processes, stores or transmits Data Zoo Data that is considered “Confidential” or “Personal Confidential,” additional data protection controls may be required.

Table 12.1. Supplier Technical and Organisational Security Measures

Area	Description
Information Security & Data Privacy	The Supplier shall ensure that Information Security and Data Privacy are managed according to international information security, cyber security and data privacy standards, laws and regulations (e.g. ISO/IEC 27000 family; SOC2; GDPR; CCPA) throughout the entire supply chain.
Information Security Risk Management	The Supplier shall ensure that: 1. A Risk Management methodology, with regular risk assessments, that provides for the identification, treatment and documentation of substantive risks and vulnerabilities that may impact Data Zoo Data must be maintained 2. The Supplier shall implement measures to secure Data Zoo Data by: a) Restricting access to Data Zoo Data only on a need to know basis b) Restricting access to systems that process or store Data Zoo Data (both at rest and in transit); c) Enforcing strict access control mechanisms; and d) Enacting, where the Supplier works with service providers, on such service providers substantially the same security requirements as described in this document to protect Data Zoo Data.
Physical Security	Physical Security controls acceptable for the type of data involved must be put into operation; at any supplier location where Data Zoo Data is stored or processed. The Supplier shall ensure that all Data Zoo Data is safe from unauthorized physical access, damage, interference, loss or theft. In this regard, the supplier shall log access to system processing Data Zoo data, restrict access based on a need-to-know basis, lock the server rooms (if any), use the video surveillance

	where permitted by law, secure the equipment used to store, process and transmit Data Zoo data including wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
Access Control and system infrastructure Control	1. The Supplier shall at minimum take all practical steps to restrict anyone other than authorized individuals from accessing Data Zoo Data in any way or for any purpose not authorized by contract and the Agreement. 2. The Supplier shall document and implement procedures and policies ensuring the Supplier has sufficient protections against malware and viruses; critical System and data backup; logging and monitoring; logs retention for no less than 18 months or, where the Supplier allows the Data Zoo to download the logs, for no less than 3 months; and technical vulnerability management. 3. The Supplier shall have arrangements to protect the security of Data Zoo Data by limiting the purposes for which Data Zoo Data may be used and confirming such purposes are permitted by the Agreement; 4. The Supplier shall grant access to individuals on a need-to-know basis 5. The Supplier shall periodically conduct access review (in no less than 12 months) 6. The Supplier shall ensure that any system where Data Zoo Data are processed is secure by design. 7. The Supplier shall have a formal change management process that embodies the principle of segregation of duties.
Incident Management and Communication of Incidents	1. The Supplier should have a formal Incident Management Process and related procedures in place. 2. If a disclosure, outbreak, violation or another breach of the agreement herein (an "Incident") occurs, Data Zoo must be informed without undue delay regarding any security breaches that might have an impact on Data Zoo Data or the provided services stated in the underlying contract.
Data Retention & Transmission	If applicable and authorized by contract/Agreement, the Supplier shall: 1. Document and enforce measures to protect Data Zoo data during transmission by applying measures to secure data in transit. 2. Not store Data Zoo Data on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under a contract between the Supplier and Data Zoo. 3. At no additional charge to Data Zoo, upon Data Zoo's request or upon the termination of the Agreement, destroy all of Data Zoo's Confidential Information and Personal Information, including electronic, hard, and secured backup copies as provided for in the Agreement or, if not provided for in the Agreement, within thirty calendars (30) days after the soonest of: (a) expiration or termination of the Agreement, (b) Data Zoo's request for the deletion/de-identification of Personal Information and Confidential Information, or (c) the date when Vendor no longer needs Personal Information and Confidential Information to perform services and products under the Agreement. 4. Dispose of Personal Information and Data Zoo Data in a manner that ensures the information cannot be reconstructed into a usable format.
Business Continuity and Disaster Recovery	The Supplier shall, at a minimum: 1. Develop, operate, manage, and revise business continuity plans for each location and disaster recovery plans for each core technology in order to minimize the impact for Data Zoo to the Supplier's service or products. Such plans shall include: named resources specific to Business Continuity and Disaster Recovery functions, established recovery time objectives and recovery point objectives, back-up of critical data and systems, record protection and contingency plans commensurate with the requirements of the Agreement, store such plans securely off-site and ensure such plans are available to the Supplier as needed. 2. Adequately review and adjust its Business Continuity Plan to address additional or emerging threat sources or scenarios and provide Data Zoo with a high-level summary of plans and testing within a reasonable timeframe upon request.
Standards, Best Practices, Regulations, and Laws	In the event the Supplier processes, accesses, views, stores, or manages Personal Information or Confidential Information pertaining to Data Zoo personnel, partners, Affiliates, Data Zoo clients; or Data Zoo client employees, contractors, subcontractors, or suppliers; the Supplier shall employ Technical and Organisational Security Measures no less strict than is required by applicable global, regional, country, state, and local guidelines, regulations, directives and law.
Modification	Data Zoo reserves the right to update or modify these Information Security Requirements from time to time by posting the latest version on Data Zoo's website. Unless the Supplier provides written notification objecting to such updates or modifications within thirty (30) days of posting, the Supplier will be deemed to have accepted these changes.

13. Policy Communication

The ISMS Manager ensures all Data Zoo Staff, as well as appropriate external parties, are familiar with this Policy.

15. Breach of Policy

We will take all necessary measures to remedy any breach of this policy including the use of our disciplinary or contractual processes where appropriate.

16. Records

Records retained in support of this procedure are listed in the ISMS Document Control and Improvements Register and controlled according to this ISMS Document Control Procedure.

Glossary

AML: Refers to “Anti-Money Laundering”.
API: Refers to “Application Programming Interface”.
Audit Scope: Refers to which areas are included and which are excluded from the audit.
Audit Objectives: Refers to the purpose of the audit and what it should achieve.
Audit Criteria: Refers to which Clauses, Controls, and Policies are to be audited.
Batch: Refers to a batch process of identity verifications.
CDR: Refers to “Consumer Data Right”.
Data Zoo Data: Refers to either:
(a) the data that the verification subject, or a person acting on their behalf, provides to Data Zoo for identity verification purposes. Data Zoo provides this data to the Supplier, or permits the Supplier to access, in connection with the Agreement; or
(b) the Supplier creates or collects in connection with the Agreement; or
(c) is derived from the data listed in (a) and (b).
DMZ: A DMZ Network is a perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic.
GDPR: Refers to the European Union’s “General Data Protection Regulation 2016/679”.
CCPA: Refers to the US “California Consumer Privacy Act”.
IDU / IDU System: Refers to Data Zoo’s Electronic Identity Verification platform, encapsulating all access points such as our SOAP and REST API, and Web-Application Interface.
Hashing: Refers to the de-identification of personally identifiable information in a way that it cannot be reconstructed.
ISMS: Refers to Information Security Management System.
JAS-ANZ: Joint Accreditation System of Australia and New Zealand. (About us | JAS ANZ (jas-anz.org))
Machine: Refers to Data Zoo Employee Laptops.
MDM: Refers to “Mobile Device Management”.
OS: Refers to “Operating System”.
PII: Refers to Personally Identifiable Information. That is any information that can potentially identify an individual (including instances of inference, etc).
SOC / SOC 2 / SOC 3 : Refers to “Service Organisational Control”.
Source Data: Refers to the personal information provided by clients to Data Zoo for the purposes of Identity Verification.
Supplier: Refers to the person/organisation providing the Services to the Data Zoo under the Agreement.

REFERENCES

Legislation / Standards	Policies	
Privacy Act (1988)	Acceptable Use Policy	Information Classification and Handling Policy
General Data Protection Regulation 2016/679	Access Control Policy	Mobile Device Management Policy
California Consumer Privacy Act	Backup and Restore Policy	Pandemic BCP
Consumer Data Right Act 2019	Business Continuity & Disaster Recovery Plan	Password Policy
ISO 27001:2013	Change Management Policy	Periodic Access Review Plan
	Corrective Action Plan	Risk Treatment Plan
	Cryptographic Controls Policy	Roles and Responsibilities Register
	Data Disposal Policy	Vulnerability Management Procedure
	Disciplinary Policy	Vulnerability & Penetration Assessment Summary
	Incident Management Policy	Teleworking Policy
	Information Asset Inventory	

Change History

Version	Date	Detail	Author	Approved By
1	03/12/2018	Initial issue.	MP	TF
2	23/02/2019	Update for ISO27001.	MP	TF
3	21/08/2019	Rewrite of document.	MA/JR	TF
4	12/09/2019	Update to Data destruction section.	MD	TF
5	30/10/2019	General updates.	MA/JR/MD	TF
6	26/04/2020	Update following ISO 27001 Surveillance Audit.	MA/JR	TF
7	02/07/2020	Updated formatting and version.	MA/JR	TF
8	21/07/2020	Addressing previous client confusion.	MA/JR	TF
9	24/07/2020	Adding to Access Control Section.	MA/JR	TF
10	11/03/2021	Addition to Device Security section and glossary.	JR	TF
11	09/05/2021	Addition of Section on Acceptable use of devices and secure employee behaviour.	JR	TF
12	18/08/2021	Restructured, Updated.	JR/MA	TF
13	27/01/2022	Restructured, Updated, Added CDR, Supplier Due Diligence, Updated Data Retention, and Data Lifecycle Management.	MA	TF
14	09/03/2022	Reviewed Content, numbering and formatting; Table 12.1. Supplier Technical and Organisational Security Measures added.	MA	MD, TF