Public

Information Security Policy

Version 12 – August 2021

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. Purpose, Scope and Users

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 Data Zoo's security policies. Users of this document are all employees of Data Zoo, as well as relevant external parties. Further details and explanations can be provided by the Data Zoo Compliance Team on request.

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 – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

3. Compliance and Assurance

3.1. Compliance Framework

Data Zoo has developed a compliance framework that enables the organisation to effectively identify and manage information security, privacy, and business risks. Data Zoo ensures the security and confidentality 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 controls; and is working towards ISO 27701:2019. Data Zoo GDPR Compliance can be viewed at: https://www.datazoo.com/compliance

3.2. ISO 27001:2013 Certification

Data Zoo has designed, developed, and implemented comprehensive information security controls in our Information Security Management System (ISMS) to establish, monitor and continually improve our safeguards for the confidentiality, integrity and availability of all physical and electronic information assets. Data Zoo's 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. ISO 27001:2013 certification for other international Data Zoo offices will be obtained when COVID-19 restrictions are eased and it is safe to do so. Certification can be viewed at: https://www.datazoo.com/compliance/

3.3. SOC 2 Type 1 & 2 & SOC 3 Reports

Data Zoo has successfully 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. Data Zoo can provide a copy of the respective reports upon request.

4. Risk and Information Security

4.1. Risk Assessment

Data Zoo has adopted a straightforward risk assessment methodology; undertaking an information security risk review throughout the organisation, taking 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.

Data Zoo’s 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.

4.2. 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 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, determine the root cause of the non-compliance, evaluate the need for actions to ensure that non-compliance does not reoccur, devise a corrective action plan, and review the corrective action taken to ensure outcomes are as expected. Data Zoo undertakes quarterly vulnerability and penetration testing on all of its systems to ensure technical resilience.

In line with the ISO 27001:2013 standard, Data Zoo is subject to annual external surveillance audits, with a recertification audit every 3 years. Further, Data Zoo is subject to annual SOC 2 Type 2 audits of implemented Trust Services Criteria (TSP) as required by the framework.

4.3. Vulnerability Assessment and Penetration Testing

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

4.4. Roles and Responsibilities

Data Zoo recognises the importance of designating competent and appropriate resourcing in order to meet its compliance commitments and ensure information security and privacy. The organisation has appropriately assigned and communicated all roles and responsibilities of its compliance framework to fit and proper staff. These roles and responsibilities are documented in DZ_ISMS_Roles_and_Responsibilities.

5. Information Handling

5.1. Personally Identifiable Information (PII) Protection

Data Zoo considers Personally Identifiable Information (PII) to be the most sensitive data and of the highest information classification rating for information assets, i.e., Top Secret. Confidentiality of PII stored for transactional purposes is achieved via hashing in accordance with data classification policy and levels, wherein different hashing schemes have been developed for individual PII fields based on their classification level. Data Zoo complies with the Australian Privacy Act (1988) and adopts GDPR best practices for the management of PII.

Data Zoo ensures 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.

5.2. Data Destruction

Data Zoo has a dedicated Data Destruction policy (DZ_ISMS_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. Data Zoo provisions IDU electronic verifications via API, Batch, or the IDU Web Application.
API – all transaction logs and search summary reports are data hashed to anonomize PII immediately prior to secure storage;
Batch – all transaction logs and search summary reports are data hashed to anonomize PII prior to secure storage. Further, the result customer files are deleted from the SFTP service 24 hours after delivery; and
Web – all transaction logs are data hashed to anonomize 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 approved Data Destruction Policy.

5.3. Data & Service Integrity

Data Zoo ensures the integrity of all services and data sources through rigorous quality assurance process, consisting of both manual and automated testing processes. The automatic monitoring is done via FreshPing that allows Data Zoo to maintain an active system monitoring application which 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. The tool used is Postman Monitoring.
This testing regime reports on expected and actual results with exceptions promptly investigated by Data Zoo support staff. The aim of this testing is to ensure response structures and data formats remain consistent.

5.4. Data Life Cycle Management

Data Zoo considers privacy in all stages of the data lifecycle. It ensures that data acquisition processes are adequate to capture all data needed to perform the operation. Data is then stored and secured in an optimal manner to minimize 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. The classification scheme has five levels: as outlined in ISMS A8.2 Information Classification Policy.

After data has been used and is no longer needed, it is destroyed in accordance with DZ_ISMS_Data_Disposal_Policy. Please refer to *Table 13.1 – Data Life Cycle Management* for a summary of Data Life Cycle stages.

Stage	**Protection Procedure**
Collection/Transmission	Data is transferred via SOAP and/or RESTful web service calls via HTTPS.
Use	All sensitive data is hashed immediately so that it can never be reidentified.
Retention	We do not retain any kind of identifiable client PII as per our information classification policy.
Destruction	Data is destroyed when no longer needed.

Table 13.1 – Data Life Cycle Management

5.5. Asset Management

Data Zoo ensures that all critical assets associated with information and information processing facilities are identified and listed in the DZ_ISMS_Register_Information_Asset_Inventory, which is maintained by the ISMS Manager. Each listed asset is allocated an "owner" and assigned an information classification in line with the scheme defined in ISMS A8.2 Information Classification Policy. Data Zoo has defined and implemented a DZ_ISMS_Policy_Acceptable_Use, that details the requirements for acceptable use of assets, which all employees and contractors are informed of and required to meet. Data Zoo ensures the appropriate handling of information assets per their information classification.

6. Access Controls

6.1. Access Control Policies

Data Zoo evaluates risks relating to access controls and implements supporting controls accordingly in ISMS A9.1 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 (DZ_ISMS_Access_Provisioning_Deprovisioning), and periodic reviews of access (DZ_ISMS_Periodic Access_Review) are undertaken to ensure integrity..

6.2. System Access Control

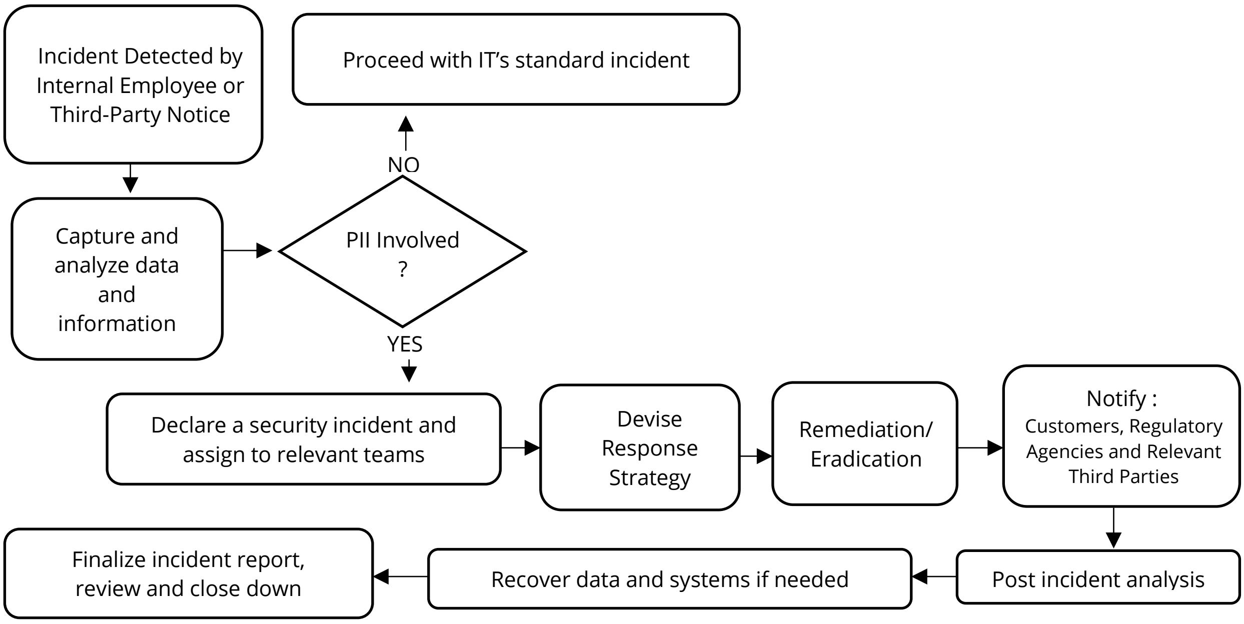
Access to Data Zoo' services is granted through the individual allocation of user rights, and requires authentication by username and password. Data Zoo has implemented a formal DZ_ISMS_Password_Policy, which specifies both the technical requirements for passwords as well as the expected procedures and practices related to password management by employees. Data Zoo manages all official passwords via LastPass, which is enforced, monitored and managed under Data Zoo MDM program. Data Zoo requires customers to supply their IP addresses for security and use of its services. Data Zoo's System will automatically IP block a Customer account if more than 10 sequential incorrect credentials are provided within a 24 hour period. Access to configuration management is only by Data Zoo Support staff and is reinforced with multi-factor authentication processes. All changes (data source access, configurations etc) to accounts are logged and monitored regularly.

7. Information Security Incident Management

Data Zoo has implemented a formal ISMS A16 Information Security 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 employees and contractors/ suppliers are required to promptly report any suspected information security events to their manager and the ISMS Manager, who then work together to complete an Incident Report Form. Data Zoo requires 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 ISMS Manager assesses the event to see if it should be classified as an incident and, where necessary, takes immediate remedial actions to alleviate the threat. The details of the incident, remediation action taken, and outcomes are recorded in a formal register for improvement and audit purposes. Figure 7.1 summarises the incident mangement workflow and response procedure:

8. Change Management

8.1. Change Management Procedures



Incident Detected by Internal Employee or Third-Party Notice
Proceed with IT's standard incident
NO
Capture and analyze data and information
PII Involved ?
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
Finalize incident report, review and close down

Figure 7.1 Incident Management Workflow

Data Zoo utilises formal procedures to address risk related to changes in systems and business circumstances. All changes are subject to the ISMS A12.1.2 Change Management Procedures, 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.

8.2. Security in Change Management

Data Zoo considers 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 developed and followed for all significant changes in Data Zoo 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 Data Zoo's IT Manager before the change is rolled out to the production environment.

8.3. System Security

Data Zoo's 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, Data Zoo 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 fail over 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.

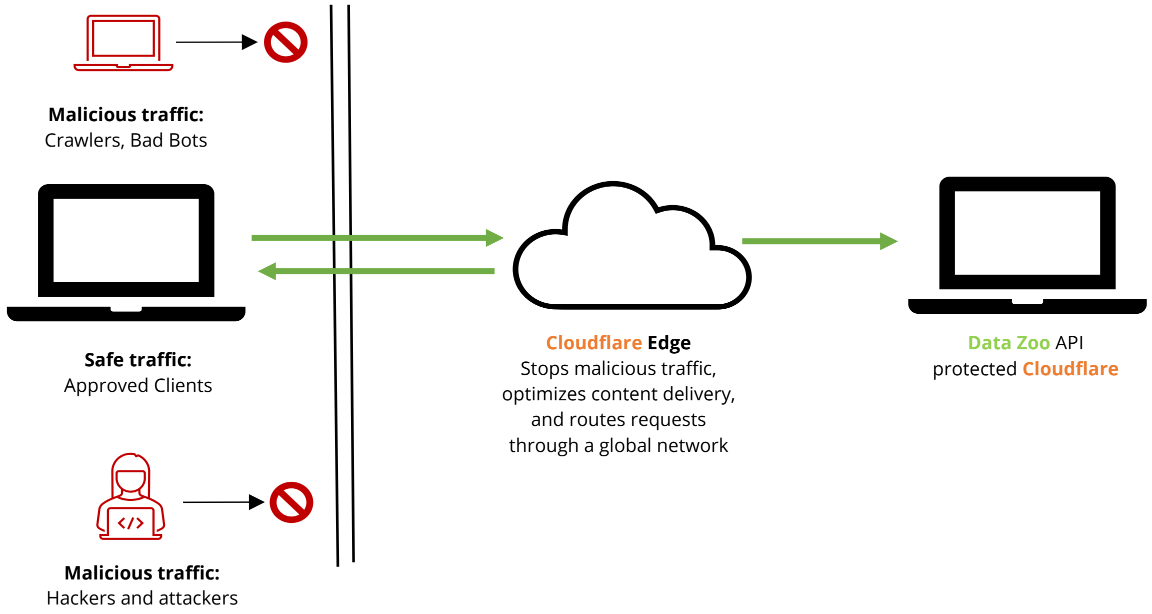


Figure 8.1. System Security

8.4. Backup and Recovery

Backup copies of information, software and system images are taken and tested regularly in accordance with a formal ISMS A12.3 Backup and Restore Policy. Data Zoo ensures that the extent, frequency, and retention period of backups reflect business requirements, security requirements, 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.

8.5. 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 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 at the time of transaction so it cannot be reidentified in any way, shape or form. For API and web users, Data Zoo logs and monitors IP addresses for each server access. Data

Zoo captures IP ranges for clients at time of signup, and validates the IPs accessing Data Zoo servers to ensure no unexpected traffic. These IP addresses/ranges are classified as business confidential information and is never accessed for a reason other than for support processes or tracability of incidents.

8.6. Test Data Management

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

9. Device Security

9.1. Device Security

All Data Zoo employee machines are enrolled into a centralised mobile device management (MDM) Program to ensure they adhere to all required technical compliance controls. Employees are restricted from installing or removing applications from their machine without appropriate IT approval and intervention, and all updates to OS, 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 to ensure 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. Data Zoo's MDM program is a managed service by a trusted and recongised third-party provider.

9.2. Acceptable Use of Devices & Secure Behaviors of Employees

All Data Zoo employees are required to acknowledge and adhere to the DZ_ISMS_Policy_Acceptable_Use, and are given formal onboarding training to be made aware of their personal responsibilities in regards to Information Security and Privacy. Data Zoo employees are required to screen lock their devices whenever stepping away, if they are in an authorized office or teleworking space. Employees are not permitted to leave their devices unattended in any other setting, such as a public place or vehicle, or with any unauthorized persons for safe keeping. Data Zoo employees must remain vigilent at all times in order to safeguard information and data and to protect the security and integrity of our IT systems, and must report any suspicious or unknown equipment or persons near Data Zoo devices to management immediately.

10. Physical Security

10.1. Physical Security and Environmental Security

The Data Zoo's Sydney office premises is securely guarded with 24 hour surveillence. Access to office is restricted to only authorized people with the provision of keys. Guests need to register at reception. The shared office space goes into lock down after 5:00 pm. During "out of office" hours the access is only through a registered fingerprint system. Appropriate physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster have been put in place. Data Zoo's additional office locations (i.e., Brisbane, NewZealand,Melbourne, Singapore, Manilla) have adequate physical security measures in to secure access to company facilities, equipment, and resources, keeping unauthorized personnel away.

Security is applied to mobile assets such as laptop computers, which are enrolled on the MDM program and managed under Data Zoo MDM program (See “9. Device Security” above). The Data Zoo 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.

10.2. Data Centres

Data Zoo utilises firewalls and encryption, which is used to protect all data and our applications. Databases have built-in security that prevent unauthorised access from malicious actors. All transactions are user and IP address logged. Data is securely stored in unconnected and independent Tier 3 physical data centres within Singapore, New Zealand and Australia, with no single point of failure and with a fully scalable world-class infrastructure. 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.

Data Zoo has 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 Data Zoo is managing data centre security or for data centre technical specifications please contact your account representative or contact us via info@datazoo.com.

11. Network Security

Network security is managed and controlled to protect 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 clearly segregated on networks.
Onsite, Data Zoo staff use protected WiFi provided by the building management. Offsite, Data staff use private protected WiFi or Personal Hotspots. The IP’s of all employees and contractors who have access to Data Zoo infrastructure, are registered and whitelisted.

12. Business Continuity Management

12.1. Business Continuity Management

Data Zoo has in place a DZ_Business_Continuity_Management and associated processes. There is a Business Continuity Plan defined and documented which explicitly states the recovery procedures required to continue and restore core services and operations in the event of a disaster. Data Zoo undertakes regular Business Continuity Testing and utilises both tabletop and technical recovery testing to test resilience to disruptions and effectiveness to restore operations. A copy of DZ_Business_Continuity_Management can be provided upon request.

12.2. Pandemic Business Continuity Management

In response to the risks presented by COVID-19, Data Zoo has set out the framework for the 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 DZ_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. A copy of the DZ_Pandemic_BCP can be provided upon request.

Figure 12.1 summarises the steps of Pandemic BCP.

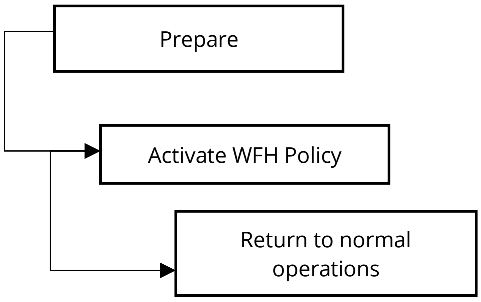


Figure 12.1. Pandemic BCP

Legal and Regulatory Compliance

12.3. Cross Border Transfer Of Information

Data Zoo's 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 Data Zoo's systems.

12.4. Insurance

Data Zoo maintains 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 reviews the insurance on needs basis or otherwise atleast once a year.

13. Policy Communication

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

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”.

GDPR: Refers to the European Union’s “General Data Protection Regulation”.

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-identificaion 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 2+ : Refers to “Service Organisational Control”.

Source Data: Refers to the personal information provided by clients to Data Zoo for the purposes of Identity Verification.

Revision History

Revision	Date	Detail	Author	Approved By
001	03/12/2018	Initial issue	MP	TF
002	23/02/2019	Update for ISO27001	MP	TF
003	21/08/2019	Rewrite of document	MA/JR	TF
004	12/09/2019	Update to 10. Data destruction	MD	TF
005	30/10/2019	General updates	MA/JR/MD	TF
006	26/04/2020	Update following ISO 27001 Surveillance Audit.	MA/JR	TF
007	02/07/2020	Updated formatting and version.	MA/JR	TF
008	21/07/2020	Addressing previous client confusion.	MA/JR	TF
009	24/07/2020	Adding to Access Control Section	MA/JR	TF
010	11/03/2021	Addition to Device Security section and glossary.	JR	TF
011	09/05/2021	Addition of Section 17. Acceptable use of devices and secure behaviours of employees.	JR	TF
012	18/08/2021	Restructured, Updated	JR/MA	TF