Zenva Pty Ltd

Information Security Policy

Securing information

GV04

Table of Contents

[Document Structure 3](#_30j0zll)

[Purpose 3](#_1fob9te)

[Scope and Applicability 4](#_2et92p0)

[Document Version Control 4](#_tyjcwt)

[Responsibility and Accountability 5](#_3dy6vkm)

[Employees/Contractors/Contractors Commitment 5](#_1t3h5sf)

[Roles and Responsibilities 5](#_4d34og8)

[Publish / Distribute IT Security Policy Document 5](#_2s8eyo1)

[Non Compliance 6](#_17dp8vu)

[Objective of Information Security Policy 6](#_3rdcrjn)

[Information Security Policy 7](#_26in1rg)

[Policy Exception 18](#_3o7alnk)

Document Structure

Zenva Pty Ltd’s information security policy suite aims to protect the confidentiality, integrity and availability of its customers and own information. To ensure that all Employees/Contractors securely handle information, the following document structure has been designed:

1. A **policy** document has many policy statements outlining Zenva Pty Ltd’s requirements and aims for supporting and governing secure handling of Zenva Pty Ltd’s information. Each policy statement is defined and approved statement of mandatory direction and intent that must be followed.
2. A **standard** is a set of requirements which have to be followed to achieve the objectives specified of each policy statement. Standards define the baseline level or controls required to comply with the policies. Note that:
	1. The word ***must*** is used to indicate mandatory requirements strictly to be followed in order to conform to the policy and standard and from which no deviation is permitted.
	2. The word ***should*** is used to indicate that the standard requirements is not mandatory, however is recommended to be implemented to meet the policy requirements.
3. A **procedure or process** is a detailed description of activities, tasks or methods followed to achieve compliance with the policy and standards.
4. A **guideline** is system specific or procedural specific instructions to achieve the procedure requirements to achieve policy compliance. This could be specific to a particular system such as email or tool and outlines how it should be used.

Purpose

The purpose of this policy is to define Zenva Pty Ltd’s requirements to protect its information and to educate all personnel to securely handle Zenva Pty Ltd and its customers’ information and protect it from unauthorised access, modification, disclosure, and destruction.

The policies and standards contained within this document are based on internationally accepted principles for information systems security. These principles are embodied in the international standard ISO/IEC 27002 for the Security of Information Systems.

Scope and Applicability

This policy applies to all Zenva Pty Ltd Employees/Contractors, including full time and part time Employees/Contractors, consultants, and other workers at Zenva Pty Ltd office and customer service sites, including all personnel affiliated with third parties.

This Policy outlines the criteria for easily classifying and protecting Zenva Pty Ltd’s and its customers information resources.

Document Version Control

| Version | Issue Date | Description of changes | Established / Updated by | Reviewed by |
| --- | --- | --- | --- | --- |
| V1.0 | 14 July 2020 | Initial Draft | Syed Qamber | Pablo |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

This policy is a living document and can be updated as determined by those responsible for updates and revisions. Ad hoc and scheduled reviews should also take place to reflect the changing requirements within Zenva Pty Ltd.

All requests for changes can be submitted to the policy owner, whom will discuss change requests with the relevant stakeholders and accept or reject the request. Following approval, the change(s) will be incorporated into this policy. The requester will be informed of the outcome

Responsibility and Accountability

Employees/Contractors/Contractors Commitment

Zenva Pty Ltd’s management is committed to have all Employees/Contractors comply with the requirements of this policy.

Roles and Responsibilities

The following Zenva Pty Ltd personnel have designated responsibilities to information security management with regard to the requirements in this policy:

| Document Criteria | Description |
| --- | --- |
| Company Head | Is responsible for the overall governance and ensuring that the right resources and solutions are in place for Employees/Contractors or users to securely handle and protect information. |
| Users | Are Zenva Pty Ltd Employees/Contractors’ members or third parties who are responsible for complying with this policy. |
| Service Providers or Third Parties | Are also responsible for complying with this policy. |

Publish / Distribute IT Security Policy Document

Publishment of this document can be provided to:-

* Regulatory authority
* Relevant personnel
* Zenva Pty Ltd Staff
* Contractors to Zenva Pty Ltd

This must be sent via printed copy of via PDF document only. This document is proprietary to Zenva Pty Ltd and can only be changed according to IT Security Policy Change Management process. The dissemination of this document is to be approved by the Company Head.

Non Compliance

All Zenva Pty Ltd Employees/Contractors, including full-time, temporary and third-party Employees/Contractors, with access to IT systems and equipment must adhere to this policy. Zenva Pty Ltd undertakes monitoring of the use of its systems and equipment.

Employees/Contractors found to have violated this policy will be disciplined as per Zenva Pty Ltd’s Human Resources policy. Corrective actions could include, but not limited to:

* Revoking or restricting any right to access or handle specific information;
* Warning or cautioning; or
* Termination of employment/ Contractors.

If Employees/Contractors behaviour constitutes a criminal offence, then appropriate legal action may be taken. Breaches to this policy can be reported to Human Resources or Company head in writing.

Third parties found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

Objective of Information Security Policy

The Zenva Pty Ltd Information Security Policies in this Manual aim to manage Information-related security risks by:

* Defining information security principles to be adopted and followed within Zenva Pty Ltd.
* Defining the roles and responsibilities of IT users, systems administrators and other stakeholders.
* Providing a framework for implementing information security management at Zenva Pty Ltd.
* Raising awareness of security risks relating to information and IT infrastructure used by Zenva Pty Ltd.

Information Security Policy

### Protection of Information

**Policy:** Zenva Pty Ltd must have a formal approach to identify and protect the Confidentiality, Integrity and Availability of all its information assets. This will ensure safeguard of its information and that of its customers, the continuity of its operations, and minimize the impact of should information security incidents occur.

**Standards:**

1. Zenva Pty Ltd should implement Information Security framework or strategy based on industry best practices (ISO 27001/2) to ensure secure management of all information across the organisation.
2. Zenva Pty Ltd must ensure that its information security practices must be enforceable by all Employees/Contractors by understanding the information asset type, classification and protective measures.
3. This document will also adhere to the regulations and guidelines of the respective geographical location where Zenva Pty Ltd operates.
4. Information Security measures will continue to be aligned with the Zenva Pty Ltd’s strategic goals and intended to be an enabling mechanism for information sharing, continuation of services, and reducing information-related risks to acceptable levels.
5. This policy document will be reviewed by the Information Security Team at least annually and updated as needed to reflect changes to business objectives or the risk environment. Any major or minor change will require approval from the Company head.

**Policy:** Zenva Pty Ltd must provide clear directions for safeguarding information and will implement adequate security controls to mitigate its information security risk profile.

**Standards:**

1. Zenva Pty Ltd Employees/Contractors must implement the suitable controls, which could consist of people, policies, procedure, standards, guidelines and technologies (hardware and software) to mitigate any exposure to its own or customers’ information.
2. Zenva Pty Ltd should measure the effectiveness of its controls through risk assessment (refer to Zenva Pty Ltd’s Information Risk Assessment procedure), vulnerability testing (refer to Security Testing and Maintenance policy), security audits and compliance checks.
3. Retention period for assets and data must be determined by Zenva Pty Ltd based on business and regulatory requirements. These should not be retained longer than required.
4. Event logs should be kept for a year and at least three months is available for immediate analysis.

### Information Classification, Handling and Destruction

**Policy:** Zenva Pty Ltd must classify, handle and destroy its information as per below.

**Standards:**

1. Zenva Pty Ltd’s Information Classification has three different criteria (been based on the Zenva Pty Ltd’s International criteria:

**Restricted Information:** This is information which is crucial to the effective conduct of our business activities and essential to our meeting of our business objectives. Loss or damage to this data would cause considerable loss, whether of reputation, revenue or future potential business. This data must be handled with special care and its accuracy, currency and adequacy must be protected at all times from unauthorised access, damage and deletion. Whether it stays the same or is changed in any way. It can only be used for the purpose for which it was intended and only by authorised personnel in a way which is commensurate with this classification. Some examples are:

* Usernames and Passwords
* Merchant Bank Account details
* [Employees/Contractors](#23ckvvd) payroll records

**Confidential Information:** This is information which is still business sensitive and therefore has a limitation, or restrictions placed on its access and use.

It is information which may be shared, both inside and outside the company, but has restrictions placed on who can access and how they can use it. It will include, but not be limited to, contractual documents and agreements, negotiating and tender documents and other confidential information. This will include sensitive Employees/Contractors information. Examples of confidential information include but are not limited to:

* Company confidential
* Source Code
* Audit or Risk assessment reports
* Demographic research
* Strategic plans
* Personal Information
* Phone number, address and business card of merchants
* Financial information share to regulatory authorities
* Corporate strategies
* Competitor sensitive
* Trade secrets
* Specifications

**Public Information:** Information which Senior Management has designated as open to access without special permission or authorisation.

Some examples are:

* Approved press statements
* Marketing materials
* Company name
* Zenva Pty Ltd policies which one might reasonably expect to see on a Company website.
1. All information must be handled as per the classification requirements and be labelled accordingly.

### Regulatory Compliance

**Policy:** Zenva Pty Ltd and all Employees/Contractors must abide by all applicable regulatory requirements for information security to ensure that all information security practices are adequate, consistent and avoid implications, such as monetary fines or loss of business licenses. Zenva Pty Ltd Limited (the “Company”) provides a payment service to facilitate payments between businesses and customers.

**Standards:**

1. Zenva Pty Ltd and all Employees/Contractors must abide by Information Privacy Act 2009, Right to Information 2009, IS18 Information Security, Information Security Framework, Information Management Policy Framework, Queensland and legal and regulatory requirements for information security.
2. Zenva Pty Ltd must measure compliance against all applicable standards requirements (such as ISO27001 to protect for the specific assets, supporting infrastructure and processes as required.
3. Zenva Pty Ltd must abide by any contractual information requirement entered into with third parties (e.g. customers, service providers) such as non-disclosure agreements, access procedures and acceptable uses.
4. Zenva Pty Ltd should review applicable regulatory or contractual requirements and ensure only the most relevant and application controls for securing its own and its customers’ information. If any applicable requirements could compromise Zenva Pty Ltd’s operation or reputation, it must be disputed with relevant stakeholders.

### Third-Party Management and Outsourcing

**Policy:** Zenva Pty Ltd must ensure the protection of its information and information systems through the inclusion of appropriate controls specified in all contracted Third-Party arrangements.

**Standards:**

1. Arrangements involving third party access to ARL information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the Zenva Pty Ltd security policies and standards. The following terms should be considered for inclusion in the contract:
	1. General policy on information security.
	2. Asset protection, including:
		1. Procedures to protect Zenva Pty Ltd assets, including information and software.
		2. Procedures to determine whether any compromise of the assets, e.g., loss or modification of data, has occurred.
		3. Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract.
		4. Integrity and availability.
		5. Restrictions on copying and disclosing information.
	3. Description of each service to be made available.
	4. Target level of service and unacceptable levels of service.
	5. Respective liabilities of the parties to the agreement.
	6. Responsibilities with respect to legal matters, e.g., data protection legislation.
	7. Responsibilities regarding hardware and software installation and maintenance.
	8. Any required physical protection controls and mechanisms to ensure those controls are followed.
	9. Controls to ensure protection against malicious software and vulnerabilities.
	10. Arrangements for reporting, notification and investigation of security incidents and security breaches.
2. Outsourcing arrangements must address the risks, security controls and procedures for information systems, networks and / or desktop environments in the contract between the parties.
3. All third-party services delivered to Zenva Pty Ltd must be regularly monitored and reviewed.
4. Independent audit reports such as SOC 2 Report provided by the suppliers must be reviewed at least annually.
5. The focus of the report must include security controls that are relevant to Zenva Pty Ltd such as Patch Management, Vulnerability Management, Identity and Access Management, Logging and Monitoring, System Hardening, Data Protection.
6. Any changes to services provided by a third party must be managed by Zenva Pty Ltd. This will include provisioning of services, changes to existing services and new services. Evaluation of the risks to Zenva Pty Ltd must be undertaken based on the criticality of the system and the impact of the change.

### Information Asset Management

**Policy:** Zenva Pty Ltd’s information assets must only be used for business purposes and to deliver the services required for its customers. Zenva Pty Ltd’s information assets can be electronic or hardcopy (for example, systems, portable devices, applications, paper based documents).

**Standards:**

1. Information assets should be located on premises within Zenva Pty Ltd’s facilities or on cloud managed by third parties. When working with the Australian government, all user data must be stored in Australia.
2. Refer to Zenva Pty Ltd’s Acceptable Use policy for further information on prohibited use and limited personal use of IT resources.
3. Zenva Pty Ltd’s IT head is the asset owner and ensures all assets are classified and controls are implemented to protect sensitive information.

### Personnel Security (Human Resources)

**Policy:** Zenva Pty Ltd must ensure that information security is managed throughout the recruitment life cycle through the activities undertaken in hiring, ongoing management and termination of Employees/Contractors.

**Standards:**

1. Information Security Policy must be read and signed by all users who are granted access to Zenva Pty Ltd’s assets. For example during the new Employees/Contractors or contractor recruitment and thereafter on an annual basis to ensure ongoing acceptance by Employees/Contractors.
2. Zenva Pty Ltd reserves the right to disclose any information or users’ actions without prior consent from the user in instances where there is a legal requirement.
3. Zenva Pty Ltd must perform adequate background checks on Employees/Contractors prior to commencing employment with a third party.
4. Third party Employees/Contractors (e.g. contractors) must also be subject to background checks prior to accessing Zenva Pty Ltd’s systems.

### Information Security Awareness

**Policy:** Zenva Pty Ltd must ensure that all relevant policy, procedure, standard and guidelines applicable to protecting its own and customers’s information are communicated to all relevant Employees/Contractors and users.

**Standards:**

1. All Zenva Pty Ltd personnel must formally acknowledge their responsibilities to secure, handle and protect Zenva Pty Ltd and its customers’ information.
2. Zenva Pty Ltd must communicate any new or updated policies or procedures to ensure all Employees/Contractors can easily access and are aware of the updates.
3. Zenva Pty Ltd must provide ongoing training and awareness related to information security at least annually.
4. Security training must be provided on an annual basis. It can be computer based, team meeting, quiz etc.
5. Attendance of training and awareness programs should be maintained by the HR team to ensure refresher training is undertaken on an annual basis.
6. All Zenva Pty Ltd personnel must formally acknowledge that they have read and understood the security policy and procedures at least annually.

### Physical and Environmental Security

**Policy:** Zenva Pty Ltd’s site must be protected from unauthorised access or damage as these host the most valuable assets to its business, its Employees/Contractors, and secondly, the information and knowledge, about its own business and its customers.

**Standards:**

1. Unauthorised individuals may socially engineer into a Zenva Pty Ltd facility, pretending and tricking Employees/Contractors to allow them access to Zenva Pty Ltd’s sites and try to obtain access to classified systems and information. Zenva Pty Ltd’s Physical Access Control and Monitoring process, which includes the Visitor Handling process, must be followed to prevent this occurring.
2. All third-party personnel entering critical areas must be escorted and their entry and exit logged.
3. All entry and exit points shall be identified and controlled.
4. All secure areas shall be controlled by an access control card system, keys or biometric readers.
5. All third-party personnel entering critical areas must be escorted and their entry and exit logged.

### Equipment Security

**Policy:** Zenva Pty Ltd’s equipment, hardware and cabling, must be protected to prevent interference with its functionality which supports the daily operations of its business.

**Standards:**

1. Zenva Pty Ltd’s equipment must be securely protected as per the Physical Security policy.
2. Zenva Pty Ltd’s equipment or media which store, process or transmit restricted data must be handled as per the classification scheme.

### Anti-malware and Endpoint Security

**Policy:** Zenva Pty Ltd must implement endpoint security controls to prevent introduction of malicious code to protect its systems and applications.

**Standards:**

1. Zenva Pty Ltd must deploy, and maintain up to date, antivirus and anti-malware software to prevent the outbreak or infection of viruses and other malicious software (e.g. adware, spyware).
2. Outbreak of virus or malware incidents must be managed as per Zenva Pty Ltd’s Incident Management policy and procedure.

### Patching and Vulnerability Management

**Policy:** Zenva Pty Ltd must ensure that all applications and systems managed by Zenva are assessed for vulnerabilities and are patched in a timely manner to ensure the protection of its information and information system.

**Standards:**

1. The Application Team must be responsible for executing the patching process.
2. An automated patch management solution where possible must be installed to automate the patching process.
3. All system components must be patched for known security vulnerabilities within 30 days. However, all critical patches must be installed within 72 hours of the release.
4. Patches must be tested thoroughly in a test environment to ensure that it doesn’t cause any system issue before deploying the patch on production machines.
5. The Application Team must subscribe for security bulletins to receive latest security vulnerability updates such as Stay Smart Online, Microsoft Security Bulletin, etc.
6. Monthly executive reports must be maintained by the Application Team showing the patch status of all applications, services and plugins.
7. Applications, services and plugins that are no longer supported by their vendors must be updated to a vendor supported version or replaced with an alternative vendor supported version.
8. Vulnerability assessments must be conducted at least quarterly on all services and applications managed by Zenva Pty Ltd.
9. Penetration testing must be conducted at least annually on all services and applications managed by Zenva Pty Ltd.

### Information Backup and Archive

**Policy:** Zenva Pty Ltd must ensure that all sensitive information is archived and backed up on a regular basis and that this backup is securely maintained and easily accessed in the instances where information restoration is required (e.g. due to an incident or disaster).

**Standards:**

1. Zenva Pty Ltd should have a backup and archive timeframe and approach (e.g. incremental and monthly).
2. All audit trails and logs of system and user access must be backed up as per Zenva Pty Ltd’s Logging and Auditing process.
3. All archive and backup of desired data must be kept for twelve months or greater if there’s a business need otherwise it is not stored whatsoever.
4. All archived and back up information must be securely protected (e.g. encryption), specifically if it holds sensitive information it gets destroyed as per the contractual agreement.

### Access Control and Authentication

**Policy:** Zenva Pty Ltd’s Access Control policy must ensure that access management, provisioning, transferring, revoking and ongoing management is undertaken to provide users with only need to know access.

**Standards:**

1. All access to sensitive information, must be controlled to ensure the systems which store, process or transmitting this information :
	1. Accessed by users who require access
	2. Actions undertake are allowed to those whom require access
2. All access must be monitored daily and reviewed quarterly as per Zenva Pty Ltd’s Access Control policy requirements.
3. Access to Zenva Pty Ltd or its systems must be as per Zenva Pty Ltd’s User Authentication and Password Management process.
4. Password must be set as per the password Policy
5. Privileges must be set as per the job responsibility of the role and where necessary least privileges must be assigned
6. Multi factor must be installed to access sensitive information remotely

### Network and System Security Management

**Policy:** Zenva Pty Ltd’s network infrastructure and systems must be securely configured in order to protect information whilst it is stored, transmitted, accessed and modified.

**Standards:**

1. Zenva Pty Ltd’s infrastructure must be security tested to identify vulnerabilities and patched or remediated.
2. Zenva Pty Ltd’s must ensure the network devices and servers within the Zenva Pty Ltd Environment shall be configured as per Zenva Pty Ltd’s Secure Build Standards and a baseline check is conducted on a quarterly basis.
3. Zenva Pty Ltd must ensure that the network within the Zenva Pty Ltd Environment is scanned for vulnerabilities on a quarterly basis
4. All networks and servers on Zenva Pty Ltd’s network must have accurate timestamps, as per Zenva Pty Ltd’s Logging and Auditing process.
5. Zenva Pty Ltd must ensure a clock synchronisation system is implemented across the whole Environment, with a dedicated server or servers pulling the time from an established external time source.
6. All security testing of Zenva Pty Ltd’s IT resources must be performed by trained personnel, or qualified third parties.
7. Zenva Pty Ltd must prevent the disclosure of private IP addresses and routing information from the internal network to the Internet, and any disclosure of private IP addresses and routing information to external entities is properly authorised
8. Zenva Pty Ltd must protect its network infrastructure with firewall, IPS/IDS and appropriate Virtual Private network rules should be configured for business purpose only
9. Any deviation of systems from Zenva Pty Ltd’s should be assessed as per Zenva Pty Ltd’s Risk Assessment process.

### Incident Response

**Policy:** Zenva Pty Ltd must ensure that all incidents are efficiently managed and minimal impacts occur to the confidentiality, integrity and availability of its own and customers’ information.

**Standards:**

1. Zenva Pty Ltd’s incidents must be managed as per its Incident Response policy and supporting Incident Response procedure.
2. Zenva Pty Ltd should have an Incident Response team assigned to manage incidents.
3. Incident management should be continuously improved within Zenva Pty Ltd as new threats and exposures emerge in the Zenva Pty Ltd’s business and network landscape.
4. Incident Detection and Report: identification of incident and reporting it to the appropriate stakeholders in a timely manner. The reporting of the incident must be acknowledged. Relevant tools or controls can be implemented to detect for incidents, these should be specified in the Incident Response plan.
5. Zenva Pty Ltd must undertake incident reporting as per legal and regulatory requirements.

### Audit Logging and Monitoring

**Policy:** Logging must be enabled on all Zenva Pty Ltd systems, such as databases, laptops, servers, applications, Cloud services, wireless devices, in order to ensure records are available of user and system access to detect for unauthorised activity.

**Standards:**

1. All logs must include the following: user identification, type of event, date and time, success or failure, origination of event.
2. Zenva Pty Ltd must monitor its logs to detect anomalies or unauthorized activities. Logs ensure there is a record of access to review in case of an incident or breach.
3. Zenva Pty Ltd must ensure that a suitable solution is in place to detect tampering of logs.

### Secure System Development

**Policy**: Zenva Pty Ltd must ensure that information security is designed and implemented within the development lifecycle of information systems.

**Standards:**

1. Establish and maintain Secure Development practices, procedures, and tools, to ensure relevant security requirements are designed, built or onboarded, tested and ready for implementation/operation before new/changed solutions are deployed in particular:
	1. Code protection processes to ensure all code is securely handled and protected
	2. Secure coding practices that set forth secure coding and secure by design principles that all developers are required to apply when creating source code
2. Where relevant, adopt a risk-based approach for code review, based on the nature, type and size of the software or change.
3. Secure Development Training including secure coding training must be provided for all people involved in the development or testing of source code:
	1. Training must be provided by, or at minimum aligned with, a recognised industry body.
	2. Training must encompass secure coding principles and how to apply them throughout the software development process.
4. Access to all source code, development software and tools must be restricted in line with the Access Control and Authentication Policy:
	1. The use of development tools must be logged and monitored in line with the Audit Logging and Monitoring Policy.
	2. Development and modification of code must only take place in development environments
	3. Only authorised people can access source code and only from Zenva Pty Ltd managed devices that meet the security requirements.
	4. Source code must not be shared with individuals who are not authorised to access or handle source code.
	5. Unauthorised access to the authoritative source for software must be prevented, logged and monitored.
5. Source code must be stored in a Zenva Pty Ltd approved and managed source code repository:
	1. Source code must only be stored on or accessed from a Zenva Pty Ltd approved and monitored device.
	2. An accurate and up-to-date source code inventory must be maintained.
6. Test and development environments are logically or physically separate from, and incapable of interacting with production environments:
	1. Code development and code changes must only occur in development environments.
	2. Production data must not be used in testing or development environments unless testing or development environments are secured at the same level as production environments, or the information has been securely scrambled/masked or sanitised appropriately.
7. Code Analysis and Security Testing must be completed during development, in line with the criticality and risk of the asset/environment, including:
	1. Software Composition Analysis mechanisms to detect and track open-source components in the code case.
	2. Static Application Security Testing mechanisms to detect security vulnerabilities prior to deployment of in-house software applications.
8. Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.
9. When developing web applications, the OWASP Application Security Verification Standard must be followed.

### Encryption and Key Management (Cryptography)

**Policy:**  Data encryption secures information during transmission or storage, Zenva Pty Ltd must ensure that sensitive information has adequate encryption controls when required to protect the integrity of the information.

**Standards:**

1. Adequate encryption controls must be used by Zenva Pty Ltd to secure sensitive information, when it is stored or transmitted.
2. Where encryption is used, Zenva Pty Ltd must ensure that the keys are also securely managed.

### Risk Assessment

**Policy:** Zenva Pty Ltd must ensure all non-compliances, deviations, exposures and gaps are identified and managed as risks.

**Standards:**

1. Zenva Pty Ltd must identify and assess risks as per Zenva Pty Ltd’s Risk Assessment procedure. A risk assessment must occur least annually to identify threats and vulnerabilities.
2. Zenva Pty Ltd must ensure high and extreme risks are treated as a priority.
3. Zenva Pty Ltd must ensure where feasible, compensating controls and accept the residual risk after the treatment.

### Business Continuity and Disaster Recovery

**Policy:** Zenva Pty Ltd should have Business Continuity (BCP) and Disaster Recovery (DR) practices in place to ensure its services are uninterrupted and continuously available.

**Standards:**

1. Zenva Pty Ltd must ensure that services should be up and running at all times and adequate Business Continuity and Disaster Recovery practices are in place.
2. Adequate BCP and DR plans should be documented and tested on an annual basis or when required.
3. Zenva Pty Ltd should have BCP and DR plans of its own network environment and ensure Employees/Contractors are able to perform their business duties efficiently.

### Change Management

**Policy:** Zenva Pty Ltd must ensure that changes to all its systems by Zenva Pty Ltd Employees/Contractors or external parties follow a common process to ensure limited or no impact occurs to its critical information.

**Standards:**

1. All changes to Zenva Pty Ltd’s systems and network infrastructure must be assessed and approved as per Zenva Pty Ltd’s Change Management process and procedure.
2. All change requests and assessment should be kept on record for at least twelve months.
3. All changes should be assessed based on the type of change and possible impact. Back out or restoration steps should be followed in the event of a failed change and restoration should occur to the system's original state, prior to the change.

### Customer Notifications

**Policy:** Zenva Pty Ltd must ensure that customers are notified 30 days in advance before country relocation of data.

**Standards:**

1. Any relocation of user data including cloud infrastructure, user data services, and partner vendors that have access to unencrypted data, needs to be communicated to users 30 days in advance via email.

Policy Exception

Any exception to Information Security Policy related to confidential information and critical assets must be approved by the company head. Subsequently, the same would be documented and reported appropriately