# Project 1 - Smart Bike Project

Cyber Security Guidelines

**Document Creation:** 23 September, 2023. **Last Edited:** 23 September, 2023. **Authors:** Indiah Smith. **Document Code:** CSG P7. **Effective Date:** 23 September 2023. **Expiry Date:** 23 September 2024.

## Purpose and Scope of the Policy

The Cyber Security Guidelines (the Guidelines) outline cyber security standards recommended for Redback Operations. The Guidelines are intended to be read and implemented by Team Leaders and Support.

The Guidelines are prescribed for internal purposes and should be referred to as a cyber security policy. Whilst the Guidelines are not enforceable, it is strongly encouraged that compliance is exercised within the company. If the policy conflicts with legislation or law, the relevant law or legislation will take precedence. The organisation is encouraged to consult the Privacy Act 1988, the Security of Critical Infrastructure Act 2018 and the Telecommunications (Interception and Access) Act 1979 in the formation of the company. Guidance is also sought from the European framework of the General Data Protection Regulation (GDPR) where the data subjects are located in the EU.1

The company should be able to demonstrate adherence to these principles in order to protect its systems and data from cyber threats.

## Roles and Responsibilities

This section outlines the roles and responsibilities the organisation should assign to fulfil cybersecurity requirements.

### Director Roles and Responsibilities

General Managers, Chief Information Security Officers (CISO) or Chief Cyber Security Officers (CCSO) are responsible for:

* Appointing and assigning appropriate employees with the authority to carry out particular duties outlined in the Guidelines.
* Developing and implementing a cyber security plan to consider threats, risks and vulnerabilities that affect the protection of the company’s information and systems.
* Developing a risk management process.
* Implementing policies and procedures to promote the fulfilment of the Guidelines.
* Investigation and reporting on cyber security incidents.
* Overseeing the development and implementation of an effective cybersecurity plan.

## The Essential Eight

The **Australian Cyber Security Centre** (ACSC) recommends that organisations implement eight essential mitigation strategies from the Strategies to Mitigate Cyber Security Incidents to prevent adversaries from compromising systems.

| Mitigation Strategy | Description | Functionality |
| --- | --- | --- |
| **Application Control** | Blocking all application by default from running on devices and manually enabling approved programs. | Prevents attackers running unapproved programs and launching malware on the system. |
| **Patch Applications** | Vulnerability scans to identify where security fixes and patches can be applied to programs with 48 hours, and where applications can be removed which are unsupported by vendors. | Prevents exploitation of unpatched applications by attackers. |
| **Microsoft Office macro settings Configuration** | Enabling Office macros where required and restricting types of macros that can be executed. | Automated commands could be executed to allow attackers to install malicious software. |
| **User Application Hardening** | Configuration of applications that interact with the web to increase security and blocking ads. | Reduces the ability for attackers to install malicious software. |
| **Restrict Administrative Privileges** | Limiting access to certain applications and data to users to ensure only certain employees can alter security settings. | Administering control over administrator accounts increases difficulties for attackers gaining access to accounts with control over the system. |
| **Patch Operating Systems** | Application of security fixes/patches for operating systems within 48 hours and analysing data to check vulnerabilities within the system | Unpatched operating systems are vulnerable to exploitation by attackers seeking to access sensitive information. |
| **Multi-Factor Authentication** | Validating the user during the login process to ensure additional checks are carried out. | Unpatched operating systems are vulnerable to exploitation by attackers seeking to access sensitive information. |
| **Regular Backups** | Regular backups of data, software and configuration settings and regular testing of the data retention process. | Ensures data can be accessed following a cyber-attack. |

## Transfer of Data

### Monitoring Data Importation and Exportation

* Monitoring of data transfers should take place regularly to identify any unusual activities or abuse of data transfer privileges.
* Users transferring data should be held accountable for data transfers and ensure systems are secure and authorised to withhold the data.

### Data Logging

To preserve system integrity and manage data transfer privileges, employees should log all forms of data transfers and include information such as:

1. Who the data transfer was performed by;
2. What data was transferred;
3. Where the data was transferred to;
4. When the data was transferred; and
5. How the data was transferred.

## Database Systems

### Communication of Database Servers and Internet of Things

* All data communicated between database servers and cloud servers should be encrypted due to its susceptibility to being captured by an adversary.
* Wearable devices may be referred to as the “Internet of Medical Things” (IoMT) which refers to the connection of the devices to health information technology systems.

### Protection of Database Contents

Users of the database should be aware of the sensitivity associated with the contents of the database. All sensitive data collected by the wearable devices should be classified as such and protected through the use of access privileges to restrict database users’ ability to access, insert, modify or remove contents of the database in alignment with their role within the company.

## Managing Cyber Security Incidents

### Cyber Security Events

A system, service or network state indicating that a potential breach of security policy or unforeseen event has occurred.

### Cyber Security Incidents

An unexpected cyber security event resulting in compromised business operations or that has a likely effect of compromising business operations.

### Detecting Cyber Security Incidents

Appropriate data sources should be retained by the company and event logs should be utilised to detect and investigate cybersecurity events and cybersecurity incidents.

### Incident Management Policy

An incident management policy should be established to initiate a plan for detecting and responding to malicious activity and cover the responsibilities of the action plan, the allocation of resources, and guidelines for responding to cyber security events and cyber security incidents.

An incident management policy should be reviewed annually for compliance purposes.

### Security Risk Management Plan

A framework should be established to:

1. Assess and identify the most valuable assets and information held by the business;
2. Identify vulnerabilities that the organisation may be susceptible to; and
3. Handle the identified threats that may impact the company.

### Cyber Security Incident Register

A cyber security incident register should be developed to monitor activities associated with rectifying cyber security incidents and to be utilised as a tool for future risk assessments.

A cyber security incident register should contain the following data:

* Date of the occurrence of the cyber security incident.
* Date of the discovery of the cyber security incident.
* Description of the cyber security incident.
* Response to the cyber security incident.
* The person reporting the cyber security incident.

### Reporting Cyber Security Incidents

Cyber security incidents should be reported to the CISO as soon as practicable after discovery.

Legislation obligations should be consulted to determine reporting requirements of cyber security incidents to the authorities, customers or the public.

### Reporting Cyber Security Incidents to the ACSC

Cyber security incidents should be reported to the Australian Cyber Security Centre (ACSC).

## Responding to Cyber Security Incidents

### Handling Data Spills

In the event of a data spillage, the company should provide information about this incident to data owners and enforce access restrictions to the data.

Users should be informed about the appropriate course of action to take in regards to containing their data.

### Handling Malicious Code Infections

All infected systems should be isolated and scanned by an antivirus software to recover the data.

If the infection cannot be removed, the system should be restored to a known good backup.

## Securing Personal Information

Personal information refers to information or an opinion about an identified individual, or an individual who is reasonably identifiable.2

Sensitive information is defined in s 6(1) of the Privacy Act 1988 (‘Privacy Act’). The data collected by the mobile app should be subject to the requirements where it satisfies the elements of personal or sensitive information. Exercise metrics such as duration, intervals, distance, resistance and threshold is not considered “health information” and the privacy policy should communicate to users all the ways their data will be used. Users should be provided with an opportunity to opt-out at any time.

Default protections should be private by default and users should physically have to adjust settings to enable their data to be shared and control how it may be used.

The mobile app should be set up with two-factor authentication to ensure a code is generated and sent to a trusted device before it can be accessed.

The 13 Australian Privacy Principles (APPs) are contained under s 28(1) of the Privacy Act and provide regulations on how personal information should be handled.

* The company should take active measures to ensure personal information is secured and consideration should be given as to whether they are permitted to retain the information under APP 11.
* The company should take reasonable steps to ensure personal information is protected from misuse, interference and loss, in addition to authorised access, modification and disclosure under APP 11.1. These reasonable steps include the development of adequate cyber-security practices to meet the privacy protection requirements.
* The company should take reasonable steps to ensure personal information is destroyed or de-identified where it is no longer necessary for any purpose for which it may be used or disclosed under the APP 11.2.
* The company should collect the minimal amount of personal information that is reasonably necessary to carry out its functions or activities under APP 3.
* The company should secure personal information in adherence with APP 1 by implementing procedures relating to internal practices, processes and systems, governance, and any dealings with third-party providers that go beyond the scope of technical security measures.
* If the company provides personal information to a cloud service provider for the purpose of storage of data and providing access to the personal information, this will constitute the use of personal data by the company in the following circumstances:
  + A binding contract exists between the entity and the provider to handle the personal information in limited circumstances;
  + The contract requires any subcontractors to agree to the obligations provided in the contract; and
  + The contract specifies that the company has control over how the information is handled by the provider including whether the company has the right to access, change or retrieve the information, who will have access, the security mechanisms involved in the storage of personal information and whether the information can be retrieved or permanently deleted by the company following termination of the contract.

### Consent Requirements

Consent is required as authority for the company to handle consumer information in a particular way (APPs 7.3, 7.4 and 8.2(b)).

* Consent should be express or implied (s 6(1)). Express consent must be given explicitly orally or in writing. Implied consent is inferred from the conduct of the individual and the circumstances in which it is given. The company should opt to source express consent from individuals when obtaining health and biometric data (APP 3.3). Users must have the ability to customise or disable their devices in accordance with their preferences and requirements.
* The elements of consent that must be fulfilled are as follows:
  + The individual must be adequately informed prior to providing consent;
  + The consent must be given voluntarily;
  + The individual must be capable of understanding and communicating the consent; and
  + The consent must be current and specific.
* When transmitting the data through IoT, the company should make efforts to:
  + Communicate who will be processing the data and their core responsibilities;
  + Communicate how the data will be used from the point of sale and on set-up; and
  + Communicate information in specific increments of time.
* Prior to using the device, the user should provide consent to the Terms and Conditions and Privacy Policy indicating how their data will be used.
* Informed consent should be obtained upon change to the health of the individual, or the technical system.
* Where data is used for a secondary purpose unrelated to the primary purpose, an individual should provide additional consent and be informed as to how their data is being collected and communicated.

### De-Identification Requirements

Personal identification is de-identified ‘if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’ (s 6(1)).

Information must be de-identified by removing or altering information that identifies an individual or is reasonably likely to and includes:

1. Removing personal identifiers such as names, address, date of birth or other identifying information.
2. Removing or altering information that may allow an individual to be identified.

### Anonymisation, or Pseudonymisation of Data

Personal identification data must be able to be transformed in a manner that prevents any person with unauthorised access from tracing it back to an individual.

### Rights of Data Subjets

Data subjects may exercise any of the following rights at any time in relation to the protection of data.

* Right of access to their data and knowledge of whether it is being processed.
* Right to rectification where data is inaccurate and the individual may request for their data to be corrected.
* Right of erasure to restrict the data from being processed.
* Right to be informed in a clear and concise manner prior to the collection and use of data.
* Right to object meaning that data subjects can express if they do not want their personal data to be processed.
* Right not to be subject to a decision based on automated processing.

## Security and Privacy of VR

Cybersecurity concerns surrounding IoT devices are applicable to virtual reality headsets. The regulations encapsulating virtual reality are currently not administered in the law. However, these systems are subject to ethical and privacy implications and cyber security foundations should be applied when using VR systems.

* Users should implement the following safeguards when using the VR system:
  + Devices should be kept up to date and security patches should be applied;
  + Application software should be kept up to date;
  + A VPN should be used when the device is online;
  + Apply caution when disclosing personal information; and
  + Review privacy policies to understand how the data is being collected and used.

## Physical Security

This section outlines the physical protections that should be implemented to safeguard people and assets to comply with the Work Health and Safety Act 2011 and meet cyber security standards. These protections should be proportionate with the assessed sensitivity or risk of damage or loss.

### Physical Access to Systems

A security zone should be established and systems should be secured in premises that have been assessed by the physical security certification authority and meet appropriate standards to secure the sensitive data appropriately.

### Physical Access to Devices and Servers

* The company should have a separate server room to secure network devices and servers with appropriate keys to control access to this room.
* Physical security such as enclosures or security containers should be implemented to prohibit unauthorised access or damage to equipment.
* Workstations and keyboards should not be visible to people outside of the premises and measures such as privacy films should be implemented to prevent observation from unauthorised people.
* The company must securely dispose of physical assets.

## Securing ICT Equipment

ICT equipment should be secured when it is not in use and this may be achieved through security containers, sanitisation of memory upon shutdown or encryption of hard drives.

## Notification Requirements

Where an data breach incident occurs that is likely to compromise the rights of an individual, they must be notified immediately, and the relevant regulatory body must be informed within 72 hours.

### Nofifiable Data Breaches Scheme

* Under the Notifiable Data Breaches (NDB) scheme, companies under the Privacy Act must undertake an assessment where there has been a data loss or unauthorised access to or disclosure of personal information.
* The company must notify the OAIC where the incident is likely to result in harm to an individual.

## MQTT Security Practices

To secure MQTT communications, **TLS certificates** should be installed on the MQTT Broker. These certificates ensure that data transmitted between the client and the broker is **encrypted** and not delivered in plain text. Authorisation methods and access permissions should be implemented to ensure only authorised users or devices can access certain data. This can be done through access control lists (ACLs) or role-based access control (RBAC).