Electronic Security Biometrics and Master Key Systems

Business Name:		ABN:	
Business Address:			
Contact Person:	Phone:	Email:	

THIS RISK ASSESSMENT IS APPROVED BY THE PCBU OF THE PROJECT

Under the Work Health and Safety Regulation (WHS Regulation), a person conducting a business or undertaking (PCBU) is required to ensure that a RISK ASSESSMENT is prepared before the proposed work starts.

Full Name:		
Signature:	Title:	Date:

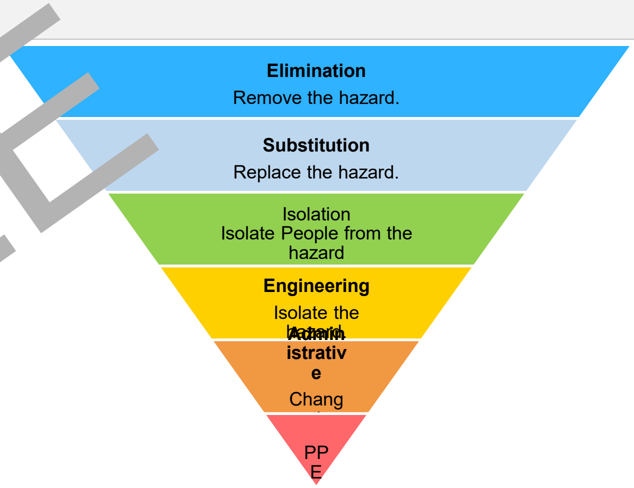
CLIENT OR PRINCIPAL CONTRACTOR DETAILS

Client:	SCOPE OF WORKS
Project Name:	
Project Address:	
Project Manager:	
Contact Phone:	
Date Risk Assessment supplied to Project Manager:	

RISK MATRIX

LIKELIHOOD	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CATASTROPHIC	SCORE	ACTION
ALMOST CERTAIN	3 HIGH	3 HIGH	4 ACUTE	4 ACUTE	4 ACUTE		
LIKELY	2 MODERATE	3 HIGH	3 HIGH	4 ACUTE	4 ACUTE	4A ACUTE	DO NOT PROCEED
POSSIBLE	1 LOW	2 MODERATE	3 HIGH	4 ACUTE	4 ACUTE	3H HIGH	Review before work starts
UNLIKELY	1 LOW	1 LOW	2 MODERATE	3 HIGH	4 ACUTE	2M MODERATE	Ensure control measures in place.
RARE	1 LOW	1 LOW	2 MODERATE	3 HIGH	3 HIGH	1L LOW	Monitor and keep records.

HIERARCHY OF CONTROLS



Risk Rating & Required Action:

4A	Stop work. The risk is intolerable. Eliminate the hazard or redesign the activity before proceeding. A Safe Work Method Statement (SWMS) or higher-level authorisation is required.
3H	Review and approve additional controls before the task starts. Senior supervisor sign-off needed.
2M	Ensure all nominated controls are in place and effective. Proceed with caution; monitor conditions.
1L	Proceed, following standard operating procedures. Monitor and keep records.

Consequence Scale:

Consequence	People (injury/illness)	Project / Assets	Compliance / Reputation
Catastrophic	Fatality or permanent total disability	project shutdown	Significant regulator intervention; criminal prosecution
Major	Serious injury/illness (hospital > 5 days)	critical delay	Improvement notice; major media coverage
Moderate	Medical-treatment injury; lost-time > 1 day	moderate delay	Minor breach; adverse client comment
Minor	First-aid only, no lost time	negligible delay	Isolated non-conformance
Insignificant	No injury	no schedule impact	Deviation caught and corrected on site

Notes on Hierarchy of Controls:
Remember to apply controls in the preferred order shown by the coloured pyramid:

1. **Eliminate**
2. Substitute
3. Isolate
4. Engineering
5. Administrative
6. PPE

Always document **why** a lower-order control is accepted if elimination or substitution is not reasonably practicable.

aligned with Safe Work Australia's Managing the risk of fatigue at work *(2023) and ISO 45001:2018 clauses 6–8.*

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
1. Governance, Legal Compliance & System Ownership	• Unclear ownership of electronic security and master key systems leading to unmanaged risks • Non-compliance with WHS Act 2011, WHS Regulations and relevant Australian Standards (e.g. AS 2201, AS/NZS ISO 31000, AS 4145 series) • Lack of governance framework for approving changes to locks, biometric systems and access hierarchies • Inadequate understanding of privacy, surveillance and data protection obligations for biometric and access-control data • Failure to integrate security risk management into broader organisational WHS and risk governance • Inadequate budgeting and resourcing for secure system design, maintenance and upgrades	4A	• Establish a formal Security & Access Governance Policy endorsed by senior management covering biometrics, master key systems, electronic locks and forensic locksmithing data • Define clear system ownership with documented roles and responsibilities (e.g. System Owner, Security Manager, WHS Manager, ICT Owner, Facilities Manager) • Align system design and risk management with WHS Act 2011, WHS Regulations, AS/NZS ISO 31000, ISO 27001, and applicable Australian Standards for locking and access control • Implement a documented change management procedure for any modification to master key hierarchies, electronic access rights or biometric templates • Include electronic security and master key risks on the organisational risk register with periodic review and reporting to the Executive and WHS Committee • Undertake periodic independent security/WHS audits of governance arrangements and implement corrective actions • Integrate security system governance with privacy and information security policies, including clear position statements on biometric data collection and use	3H
2. System Design & Master Key Architecture	• Poorly designed master key systems creating excessive access privileges and uncontrolled master keys • Overly complex keying hierarchies increasing likelihood of design errors and unintended access paths • Lack of security zoning leading to inappropriate access to high-risk or high-value areas • Absence of fail-safe and fail-secure design principles for electronic and biometric locks • Inadequate separation of duties between designer, installer and system administrator • Design decisions that compromise safe emergency egress or conflict with fire safety requirements	4A	• Develop a documented Security Design Brief that defines security zones, access hierarchies, emergency egress and interface with fire systems • Engage qualified locksmiths and electronic security designers experienced in master key and biometric system design compliant with relevant Australian Standards • Apply the principle of least privilege in master key architecture and electronic access profiles, limiting master keys to genuinely essential personnel • Implement a formal design review and approval process involving WHS, fire safety, facilities and ICT representatives prior to implementation • Standardise on lock types, cylinders and digital platforms that support high-security key profiles and audited electronic control • Ensure integration design considers fail-safe vs fail-secure requirements, emergency override, and compliance with building and fire codes • Maintain configuration documentation (schematics, keying charts, access matrices) in a secure and version-controlled repository	2M
3. Access Control Policy, Role-Based	• Lack of formal access control policy resulting in ad hoc allocation of keys, fobs and biometric profiles	4A	• Implement a formal Access Control Policy defining criteria for access, role-based profiles, approval authorities and review cycles	2M

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
Permissions & Key Levels	• Excessive or inappropriate access granted to contractors, temporary staff or visitors • No clear process for approving, reviewing and revoking physical and electronic access rights • Inadequate segregation between high-risk areas (e.g. plant rooms, server rooms, evidence stores, drug safes) and general areas • Reliance on informal verbal approvals for access level changes • Failure to remove or downgrade access after role changes, termination or contractor demobilisation		• Develop role-based access matrices linking job roles to specific zones, master key levels and electronic permissions • Require documented, manager-level approval for all new access, changes and deletions using a standardised access request workflow • Conduct scheduled access rights reviews (e.g. quarterly) to confirm ongoing need for all keys, cards and biometric credentials • Apply stricter approval, vetting and time-limited access for contractors, visitors and third parties, including after-hours restrictions where applicable • Introduce expiry dates for temporary and contractor access credentials with automatic deactivation • Ensure offboarding procedures include mandatory return and deactivation of all keys, fobs and biometric profiles with audit evidence retained	
4. Security of Keys, Credentials & Forensic Locksmithing Data	• Loss, theft or duplication of physical keys or master keys resulting in uncontrolled access • Unauthorised use or disclosure of forensic locksmithing data and key bitting information • Inadequate secure storage for key blanks, restricted key profiles and programming devices • Poor inventory control over keys, cylinders, core inserts and electronic credentials • Insider threat exploiting privileged knowledge of key systems and lock configurations • Unencrypted or poorly protected digital records of key codes and lock mappings	4A	[redacted]	2M
5. Biometric Systems Design, Reliability & Safety Integration	• Biometric systems (fingerprint, facial, iris) failing and preventing safe entry or emergency egress • False acceptance or false rejection leading to security breaches or operational disruption	4A	[redacted]	2M

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
	• Biometric devices installed in locations that create congestion, queuing or manual handling hazards • Inadequate consideration of persons with disability or injury who cannot reliably use biometric readers • Dependency on single biometric factor without backup authentication methods • Poor integration between biometric systems and fire/emergency control systems		[redacted]	
6. Electronic & Digital Lock Configuration, Reprogramming & Reset	• Incorrect configuration or reprogramming of electronic locks leading to lockouts or uncontrolled access • Use of default passwords, weak PINs or insecure programming tools • Uncontrolled resetting of electronic locks or master code changes without authorisation or documentation • Firmware or software errors causing locks to fail in an unsafe state • Inadequate version control and change tracking for lock programming files and access control rules • Remote compromise of digital locks due to insecure network connectivity or cloud management portals	4A	[redacted]	2M
7. Cybersecurity & Networked Security System Resilience	• Cyber intrusion into networked locks, biometric controllers or access control servers • Ransomware or malware affecting the availability or integrity of access control data • Insecure remote access channels for locksmiths, integrators or administrators • Lack of coordination between ICT security and physical security management	4A	[redacted]	2M

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
	• Unpatched vulnerabilities in lock firmware, management software or mobile apps • Inadequate logging, monitoring and incident detection for security system activity		[redacted]	
8. Master Key System Set-Up, Lock Reprogramming & Re-Key Projects	• Project mismanagement during large-scale master key set-up or re-key works creating periods of uncontrolled access • Inadequate verification of new key hierarchies before issuing keys and enabling new locks • Poor coordination between physical works, electronic permissions and communication to building occupants • Failure to document and update master key charts and access matrices after reprogramming or re-keying • Uncontrolled retention of old keys, cylinders or codes following system changes • Work sequencing that temporarily undermines fire safety, emergency response or WHS controls	4A	[redacted]	2M
9. Maintenance, Inspection & Servicing of Locks and Biometric Devices	• Inadequate preventative maintenance leading to lock failures or access issues • Biometric devices degrading in performance due to environmental conditions, contamination or wear • Reliance on reactive call-outs without trend analysis of failures or recurring defects • Unauthorised or unqualified personnel performing lock servicing or reprogramming • Missed inspections on critical doors such as fire exits, secure stores and plant rooms	3H	[redacted]	2M

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
	• Improper reassembly or calibration during servicing leading to malfunction or security compromise		[redacted]	
10. Incident, Breach & Fault Reporting, Investigation and Response	• Delayed or inconsistent reporting of access control failures, security breaches or near misses • Lack of structured investigation into repeated lock faults or unauthorised access incidents • Poor coordination between WHS, security, facilities and ICT when managing incidents • Inadequate temporary controls after a suspected compromise of keys, codes or biometric data • Failure to notify affected parties or regulators where breaches have WHS or privacy implications • No systematic capture of lessons learnt to improve designs, procedures and training	3H	[redacted]	2M
11. Competency, Training & Authorisation of Personnel	• Personnel administering master key and biometric systems lacking formal training or competency • Over-reliance on single individuals with critical system knowledge (key-person risk) • Inadequate induction for staff and contractors on access procedures and emergency arrangements • Unauthorised staff performing reprogramming, resetting or forensic locksmithing activities • Lack of awareness of WHS and privacy obligations relating to biometric and access-control data • Human error in data entry, enrolment, key issue or permission changes due to poor training	3H	[redacted]	2M

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
12. Privacy, Consent & Ethical Management of Biometric and Access Data	• Collection and storage of biometric data without informed consent or lawful basis • Misuse of access logs and biometric records for purposes unrelated to WHS or security • Failure to meet Privacy Act 1988 and APP requirements regarding sensitive information • Excessive retention of access and biometric data beyond justified timeframes • Insufficient transparency with workers about monitoring practices and data usage • Inadequate de-identification or destruction of biometric data on termination or system change	3H	[redacted]	1L
13. Business Continuity, Emergency Access & System Failure Planning	• Inability to safely evacuate or gain emergency access due to system failures, power outages or network issues • Overdependence on electronic or biometric systems with no robust manual fallback • Loss of access-control server or database, preventing changes to permissions during an emergency • Locked or inaccessible critical plant rooms during WHS incidents • Emergency services unable to gain timely access due to complex master key arrangements or digital locks • Poorly documented or untested emergency override and continuity procedures	4A	[redacted]	2M
14. Change Management, Upgrades & Transition to Digital Locks	• Uncontrolled or rushed upgrades to digital and smart locks introducing new vulnerabilities	3H	[redacted]	2M

JOB STEP	POTENTIAL HAZARDS	IR	CONTROL MEASURES	RR
SPECIFIC WORK STEPS	HAZARDS THAT MAY ARISE	INITIAL RISK	SPECIFIC MEASURES TO BE PUT IN PLACE TO ELIMINATE OR CONTROL THE RISKS	RESIDUAL RISK
	• Lack of stakeholder engagement when transitioning from mechanical to digital or biometric systems • Inadequate testing of new platforms, apps or cloud integrations before go-live • Incompatibility between new digital locks and existing WHS, fire or security systems • Legacy systems and shadow systems left operational, causing confusion and security gaps • User resistance or workarounds due to poorly managed change, increasing unsafe behaviours		[redacted]	
15. Contractor, Vendor & Third-Party Management	• Contractors and vendors having excessive or unmanaged access to secure areas, key data and programming tools • Lack of WHS and security vetting for locksmiths, integrators and software vendors • Inadequate contractual controls regarding confidentiality, data security and incident reporting • Unsupervised after-hours work that bypass normal controls and approvals • Poor documentation handover after installations, servicing or system changes • Dependence on a single external provider for critical knowledge and system support	3H	[redacted]	2M

EMERGENCY RESPONSE – CALL 000 FOR EMERGENCIES

Ensure to have an Emergency Management Plan in place as well as adequate numbers of trained first aid staff with easy access to fully stocked first aid kits, rescue equipment, material safety data sheets, adequate access to emergency communication equipment and fire-fighting equipment suitable for all classes of fire and ignition sources.

LEGISLATIVE REFERENCES

RELEVANT LEGISLATION AND CODES OF PRACTICE. DELETE THE LEGISLATIVE REFERENCES OF ANY STATE THAT ARE NOT APPLICABLE

Queensland & Australian Capital Territory
Work Health and Safety Act 2011
Work Health and Safety Regulations 2011
Legislation QLD: https://www.worksafe.qld.gov.au/laws-and-compliance/work-health-and-safety-laws
Codes of Practice QLD: https://www.worksafe.qld.gov.au/laws-and-compliance/codes-of-practice
Legislation ACT: https://www.worksafe.act.gov.au/laws-and-compliance/acts-and-regulations
Codes of Practice ACT: https://www.worksafe.act.gov.au/laws-and-compliance/codes-of-practice

New South Wales
Work Health and Safety Act 2011
Work Health and Safety Regulations 2025
Legislation NSW: https://www.safework.nsw.gov.au/legal-obligations/legislation
Codes of Practice NSW: https://www.safework.nsw.gov.au/resource-library/list-of-all-codes-of-practice

Northern Territory
Work Health and Safety (National Uniform Legislation) Act 2011
Work Health and Safety (National Uniform Legislation) Regulations 2011
Legislation NT: https://worksafe.nt.gov.au/laws-and-compliance/workplace-safety-laws
Codes of Practice NT: https://worksafe.nt.gov.au/forms-and-resources/codes-of-practice

South Australia
Work Health and Safety Act 2012 (SA)
Work Health and Safety Regulations 2012 (SA)
Legislation for SA: https://www.safework.sa.gov.au/resources/legislation
Codes of Practice for SA: https://www.safework.sa.gov.au/workplaces/codes-of-practice#COPs

Tasmania
Work Health and Safety Act 2012
Work Health and Safety (Transitional and Consequential Provisions) Act 2012
Work Health and Safety Regulations 2012
Work Health and Safety (Transitional) Regulations 2012
Legislation for TAS: https://worksafe.tas.gov.au/topics/laws-and-compliance/acts-and-regulations
Codes of Practice for TAS: https://worksafe.tas.gov.au/topics/laws-and-compliance/codes-of-practice

Details of permits, licenses or access required by regulatory bodies (add or delete as required):

- Permits from local council
- Authorisation to commence work
- Any required documents.

Victoria
Occupational Health and Safety Act 2004
Occupational Health and Safety Regulations 2017
Legislation VIC: https://www.worksafe.vic.gov.au/occupational-health-and-safety-act-and-regulations
Codes of Practice VIC: https://www.worksafe.vic.gov.au/compliance-codes-and-codes-practice

Western Australia
Work Health and Safety Act 2020
Work Health and Safety Regulations 2022
Legislation Western Australia: https://www.commerce.wa.gov.au/worksafe/legislation
Codes of Practice WA: https://www.commerce.wa.gov.au/worksafe/codes-practice

Safe Work Australia Links
Law and Regulation (All States): https://www.safeworkaustralia.gov.au/law-and-regulation
Model Codes of Practice: https://www.safeworkaustralia.gov.au/resources-publications/model-codes-of-practice

Model Codes of Practice

- Managing noise and preventing hearing loss at work
- Confined spaces
- Labelling of workplace hazardous chemicals
- Managing risks of hazardous chemicals in the workplace
- Welding processes
- First aid in the workplace
- Managing the risk of falls at workplaces
- Hazardous manual tasks
- Managing the risk of falls in housing construction
- Managing electrical risks in the workplace
- Demolition work
- Excavation work
- Work health and safety consultation, cooperation and coordination
- Managing the work environment and facilities
- How to manage work health and safety risks
- Managing risks of plant in the workplace
- Construction work