Holcim External Facing Cyber-security Policy

Objective

This document provides a consolidated, non-confidential overview of Holcim (Australia) Pty Ltd's (**Holcim**) cyber-security and governance framework. Its purpose is to give third parties a clear understanding of our commitment to safeguarding confidential information, Business Information, Personal Information, Intellectual Property, Sensitive Information and managing data securely, reinforcing trust, and reliability in our business interactions.

Holcim follows Best Practices/Guidelines of NIST and ISO 27001 and is compliant to GDPR, and our APAC IT and Business Service Centre is certified and audited to ISO 27001:2022 standard.

Defined Terms

For the purposes of this document, the following terms have the following meanings:

Business Information means data that relates to the commercial operations, financial status, or corporate identity of a business entity rather than the identity of a natural person such as proprietary assets, trade secrets, financial statements, marketing strategies, and operational processes that do not inherently identify an individual.

Cyber Incident means an unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.

Cybersecurity means the preservation of the confidentiality, integrity, and availability of information systems and data through the continuous application of administrative, physical, and technical safeguards which encompasses the measures implemented to protect against, and respond to, unauthorised access or interference with assets as contemplated under applicable critical infrastructure legislation and the regulatory frameworks. It includes the protection of personal information in accordance with the Australian Privacy Principles and federal privacy laws, extending to both information technology and operational technology, ensuring the resilience of digital and physical processing environments against malicious activity, unauthorised use, or accidental compromise.

Data Breach means an unauthorised access or disclosure of Personal Information, Sensitive Information or Business Information, or loss of Business Information, Personal Information or Intellectual Property personal information, held by the organisation.

Intellectual Property means all statutory and other proprietary rights in respect of

copyright and neighboring rights, circuit layouts, plant varieties, and registered or unregistered designs, patents, and trade marks as recognised under Australian law and international conventions, any applications for the grant of such rights and all renewals or extensions of those rights, as well as protected trade secrets, know-how, and confidential information that confer a commercial or competitive advantage.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether the information or opinion is true or not and regardless of whether the information or opinion is recorded in a material form or not, encompasses a broad range of identifiers including a person's name, signature, and contact details, as well as technical data such as internet protocol addresses, metadata, and location signals if they can be linked to a specific person. Information or opinions inferred about an individual from their activities or preferences, any data point which allows a person to be distinguished from a group, including sensitive information such as health records, professional associations, and biometric data.

Sensitive Information means:

a) Information or an opinion about an individual's:
   i) racial or ethnic origin; or
   ii) political opinions; or
   iii) membership of a political association; or
   iv) religious beliefs or affiliations; or
   v) philosophical beliefs; or
   vi) membership of a professional or trade association; or
   vii) membership of a trade union; or
   viii) sexual orientation or practices; or
   ix) criminal record;

   that is also personal information; or

b) health information about an individual; or
c) genetic information about an individual that is not otherwise health information; or
d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
e) biometric templates.

Information Technology (IT) and Data Protection: A Secure Digital Ecosystem

Holcim's IT governance and data protection directives ensure that information is managed securely, ethically, and in compliance with global regulations.

A. IT Governance & Security

- **Information Security:** The primary objective of IT security is to safeguard the confidentiality, integrity, and availability of both Business and Personal Information. This is achieved through robust organisational and technical measures grounded in risk management.

B. Data Privacy & Lifecycle management

- Subject to Holcim's internal data handling policy:

- **General Data Protection:** All personal data is processed lawfully, fairly, and transparently. Holcim adheres to principles such as data minimisation, purpose limitation, and storage limitation.
- **Privacy by Design & Default:** Data protection measures are embedded from the start of any new services or business processes.
- **Data Retention and Deletion:** A formal framework governs the full data lifecycle. Data is retained only as long as necessary to satisfy legal, regulatory, or business requirements, and is securely deleted or archived thereafter. A formal legal hold process suspends deletion when data is required for litigation or investigations.

Cybersecurity & Controls

Holcim adopts a robust Cybersecurity framework which third parties are required to mirror and implements a dedicated cybersecurity strategy supported by a standard set of technical controls. Together, these build a resilient digital environment and enable Holcim and any third parties to actively defend against evolving cyber threats. Holcim's Cybersecurity framework is set out below:

A. Strategic Vision for Cybersecurity

- **System Availability:** Maintenance of high-availability systems to prevent operational disruption.
- **Network Integrity:** Robust protection of network perimeter to prevent unauthorised lateral movement.
- **Data Protection:** Stringent safeguarding of sensitive, proprietary and personal information.

B. Mandatory Technical & Governance Standards

- Holcim requires all third parties, customers and suppliers to implement and maintain security measures aligned with industry best practices, specifically ISO 27001, which includes but is not limited to:

- **Access & Identity Management**

  - **Multi-Factor Authentication (MFA):** Mandatory use of MFA for accessing any systems through the Internet containing Holcim data or platforms.
  - **Password Complexity:** Enforcement of strict requirements for password length and character variety.
  - **Authorised Platforms:** Prohibition of unapproved external platforms (e.g. personal Dropbox, WhatsApp, or personal email) on business related assets.

- **Governance & Audit**

  - Third parties should maintain clear ownership of security responsibilities, oversight functions and audit obligations.
  - Holcim reserves the right to verify compliance through assessments, certifications (ISO 27001/SOC 2 Type 2), or on-site inspections.

- **Proactive Cybersecurity Measures**

  Not limited to but including:

- Endpoint Protection: Use of Endpoint Detection and Response (EDR) solutions to mitigate advanced threats in real-time.
- Vulnerability Management: Systematic processes to identify and remediate vulnerabilities, complemented by regular penetration testing.
- SSDLC: Security must be embedded in every stage of the software development lifecycle for any applications provided to Holcim.

C. Incident Management & Response

- The interconnected nature of our business means a breach in any third party, customer or supplier network may be a breach of Holcim's ecosystem.

■ **Notification Timelines:**

- **48 hour Window:** A third party authorised representative must notify Holcim in writing within 48 hours of becoming aware of any actual or suspected Cyber Incident or Data Breach.
- **Immediate Action:** If a third party's suspects that a network will impact or a network has impacted Holcim's systems directly, written notification must be made immediately, that is 'as soon as possible' to allow for appropriate rectification steps to be taken by Holcim, for network disconnection and containment.

■ **Remediation & Cooperation:**

- **Root Cause Analysis:** A third party must cooperate fully in investigations and provide a detailed root cause analysis and remedial plan.

D. Individual User Access to Holcim Systems and Applications

- If the contractual agreement with any third party, requires its officers, employees, associates, agents or affilliates (not limited to but including, a consultant, contractor, or any other capacity), to gain user level base access to Holcim's systems, the third party will be required to:
  - Sign a Non-Disclosure Agreement (NDA);
  - Comply with appropriate controls provided by Holcim, not limited to but including Holcim IT User Directive as varied from time to time;
  - Be subject to a time limited, username based, login detail for their individual use only as directed under the Holcim IT User Directive as varied from time to time, which must be followed.

Compliance with clause D above, is in addition to any contractual and legal obligations set out in any contractual arrangements entered into.

Conclusion

Holcim's information security and governance posture is comprehensive, proactive, and fully embedded into our business culture. Through a multi-layered, risk-based strategy and strict alignment with internationally recognised standards, we provide our customers and third parties with confidence that Holcim is a secure and reliable choice. We believe that this foundation of trust is essential for building strong, lasting, and successful business relationships in the digital age.

Document Control		
Created by	Legal Counsel	
Reviewed by	Head of IT Holcim Australia	
Approved by	General Counsel and Company Secretary	
Version Control		
Version	Date	Details
1.0	1/06/26	Initial version of the document.

This policy is to be read in conjunction with the Holcim ANZ Privacy Policy.