

Information Security for Vendors

We take the security and privacy of our people, clients, and information seriously. We expect the same commitment from our suppliers when handling our information or accessing our systems.

When providing goods or services to us, **suppliers must:**

Protect our information

Apply appropriate technical and organisational controls to safeguard all our information (including personal, confidential, and client information) throughout its lifecycle, and ensure it is securely returned or destroyed at the end of the engagement in accordance with our instructions.

Comply with privacy and security laws

Meet all applicable privacy, data protection, and information security laws and regulations relevant to the services provided.

Notify us of security incidents

Notify us without undue delay upon discovery of any suspected or confirmed security or privacy incident involving our information and cooperate with any investigation and remediation.

Provide evidence and allow audits

Upon request, demonstrate your compliance with these requirements by providing evidence of your security and privacy controls and allowing us to verify them (for example, through security assessments or audits).

Control access and subcontractors

Ensure our information is accessed only by authorised personnel, subcontractors and third parties.

Disclose any use of AI

Inform us on an ongoing basis if you use artificial intelligence (AI) tools or systems in delivering services including any new use, change in use, or expanded use of AI, especially if our information will be processed or stored by those systems, so that any potential security or privacy risks can be properly managed. Be able to describe how Beca information enters, is processed by, stored within and exits AI systems in the service. Be able to document any 3rd party AI providers, retention periods, jurisdictions and security controls in place.

Proportionate security or privacy requirements may apply based on the nature and risk of the services provided. These will be set out in your contract and supporting documents, such as a Privacy Impact Assessment, AI Impact Assessments, Security Risk Assessment, or Data Processing Agreement.