Security Policy

As an ISO 27001 certified company, BCQ Solutions is committed to maintaining the highest standards of information security. Our Information Security Management System is designed to ensure business continuity, prevent security incidents, and protect our information assets from all identified threats, whether internal or external, deliberate, or accidental.

Data Protection

We handle sensitive customer data with the utmost care, employing stringent security measures to protect this information. Where we are involved in building and hosting apps and websites, we implement advanced cybersecurity protocols to safeguard against digital threats.

Advanced Cybersecurity and Compliance

We employ state-of-the-art cybersecurity measures, including encryption, firewalls, and intrusion detection systems, to protect our data and systems. Our policy ensures compliance with all relevant regulatory and legislative requirements, including data privacy laws.

Enhanced Employee Training and Awareness

Our employees receive comprehensive information security training, tailored to their specific roles and responsibilities, especially those handling sensitive data. This training is integral to our security posture and is regularly updated to address new threats and best practices.

Incident Response and Management

We have established robust incident response and management protocols. All breaches of information security, whether actual or suspected, are promptly reported, investigated, and addressed with appropriate corrective actions.

Supplier and Third-Party Security Management

We extend our security standards to our suppliers and third-party partners, particularly those involved data processing. We conduct regular assessments of their security measures to ensure compliance with our high standards.

Continual Monitoring and Improvement

Our commitment to information security is ongoing. We continuously monitor and improve our security practices, setting and reviewing objectives and targets to achieve continual improvement in our information security management systems.

Responsibility and Accountability

All employees, from management to staff, are responsible for adhering to our Information Security Policy. Managers are directly responsible for implementing this policy within their business areas and ensuring adherence by their staff. Every individual in the company is accountable for maintaining the security of information.

Regular Review and Policy Updates

Our Security Policy is regularly reviewed and updated to reflect the evolving landscape of information security threats and advancements in technology. This ensures that our practices remain effective and relevant.

Transparent Communication and Accessibility

We are committed to transparently communicating our security policy, objectives, and targets. This information is made accessible to all stakeholders to foster an environment of trust and awareness.

Mark Wiseman
Managing Director
April 2024