CYBER CURE+

cyber security starts with us

July 5 2023

Policies: The unsung hero of security

Cybersecurity policies are a set of guidelines and procedures designed to protect computer systems, networks, and data from unauthorised access, use, disclosure, disruption, modification or destruction.
While the specific policies can vary between organisations and jurisdictions, here are some general reasons why comprehensive cybersecurity policies are essential for an organisation.

Consistency and Standardisation

Cybersecurity policies provide a framework for consistent and standardised security practices across an organisation. This ensures that security measures are implemented uniformly, reducing the risk of gaps or inconsistencies that could be exploited by cyber attackers.

Clear Roles and Responsibilities

Policies clearly define roles and responsibilities related to cybersecurity within an organisation. This helps employees understand their specific obligations, ensuring that everyone plays a part in maintaining a secure environment

Regulatory Compliance

Compliance with industry-specific regulations and legal requirements is a critical benefit of cybersecurity policies.
By aligning policies with relevant regulations, organisations can demonstrate their commitment to data protection and avoid legal and financial penalties.

Increased Awareness & Training

Cybersecurity policies emphasise the importance of employee awareness and training. By raising awareness about potential threats, best practices and the proper use of technology, organisations can empower their employees to become the final line of defence against cyber threats.