ICT User Policy



This policy applies to the services offered by WAV incorporating all companies and subsidiaries.

We recognise that the confidentiality, integrity and availability of information and data created, maintained and hosted by WAV are vital to the success of the business and privacy of its customers. WAV views these primary responsibilities as fundamental to best business practice to ensure compliance with all applicable laws, regulations and obligations.

WAV is committed to utilise most advanced technologies for ICT security available today and understand the importance of data security, making every effort to ensure that data held on systems are fully protected.

This Security Statement forms part of the user agreement for WAV customers.

- WAV information systems are physically protected in accordance with associated risk. All data is held in accredited data centres or within the WAV offices. Physical security controls at these locations include monitoring, visitor logs, entry requirements, and/or secure dedicated rooms for hardware.
- WAV deploys next generation unified threat management firewalls across all its networks to deliver breach prevention, and threat defence. The intrusion prevention system (IPS) features sophisticated anti-evasion technology and a network-based malware protection. Other network technologies used within the business include Network Access Control (NAC), Multi Layered anti-virus, content filtering, anti-ransomware defences, file sandboxing and application control. This combination enables WAV to block sophisticated new threats that emerge in real-time on a daily basis.
- Employees are granted WAV data access based on their role and responsibilities, and must accept WAV ICT User policies. These permissions and restrictions are reviewed regularly and revoked/granted immediately.
- Password policies are enforced and are subject to complexity, expiration and lockout. Any remote access to WAV ICT resources is only permitted through encrypted connectivity (VPN), requiring multi-factor authentication.
- Our information security policies are regularly reviewed by Senior Management and made available to employees through a central communication point. Employees are required to acknowledge these policies, accept non-disclosure agreements and undergo training and awareness on privacy and security, expected business conduct, and ransomware awareness. Training is designed to adhere to all specifications and regulations applicable to WAV.
- WAV maintain and keep up to date software and firmware patches to ensure systems, applications and devices owned and managed by the Company are routinely updated with security. This vulnerability management program includes frequent scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third party, market leading Software.
- WAV business continuity plans are in place to counteract interruptions to information systems and business activities from the effects of major failures or disasters. This involves WAV data being backed on a rotating basis of full and incremental backups and verified regularly. All WAV backups are encrypted and stored within the production environment to preserve their confidentiality and integrity.

Michael Amaeshike
Managing Director