RAM UNIVERSAL LTD.

+44 (0)1455 285428
sales@ramuniversal.co.uk
Unit 20, Cottage Lane Industrial Estate, Broughton Astley, Leicestershire, LE9 6TU
ramuniversal.co.uk

Information Security Policy 2024

Introduction:

RAM Universal Ltd is committed to ensuring the confidentiality, integrity, and availability of its information assets. The purpose of this policy is to establish the framework for the protection of our information assets against unauthorised access, disclosure, modification, destruction, or disruption. We will ensure that we successfully complete Cyber Essentials in 2024.

Scope:

This policy applies to all employees, contractors, consultants, and third-party vendors who have access to RAM's information assets. This policy also applies to all equipment, facilities, and networks used to store, process, or transmit RAM's information.

Policy Statement:

Information Classification: All information assets will be classified based on their level of sensitivity and criticality. The classification levels will be used to determine the appropriate protection measures for the information assets.

Access Control:

Access to RAM's information assets will be restricted to authorised personnel based on the principle of least privilege. Access to sensitive information will be granted only to those who have a need-to-know.

Password Policy:

All users of RAM's information assets are required to use strong and complex passwords. Passwords must be changed every 90 days, and users are prohibited from sharing passwords or writing them down.

Data Protection:

RAM are committed to providing sound data protection. We will implement appropriate technical and organisational measures to protect its information assets against unauthorised access, disclosure, modification, destruction, or disruption. This includes the use of encryption, firewalls, antivirus software, and other security controls.

Incident Response:

RAM will maintain an incident response plan that outlines the procedures for identifying, assessing, containing, and mitigating security incidents. All security incidents must be reported to the appropriate personnel immediately.

Physical Security:

RAM will implement appropriate physical security measures to protect its information assets from theft, damage, or unauthorised access. This includes the use of locks, access controls, and surveillance cameras.

RAM UNIVERSAL LTD.

+44 (0)1455 285428
sales@ramuniversal.co.uk
Unit 20, Cottage Lane Industrial Estate, Broughton Astley, Leicestershire, LE9 6TU
ramuniversal.co.uk

Third-Party Vendors:

RAM will ensure that third-party vendors comply with this policy and adhere to the same level of security standards as RAM Universal Ltd. The contracts with third-party vendors must include provisions for the protection of RAM's information assets.

Training and Awareness:

RAM will provide regular training and awareness programs to all employees, contractors, consultants, and third-party vendors to ensure they are aware of their roles and responsibilities in protecting RAM's information assets.

Enforcement:

Violations of this policy may result in disciplinary action, up to and including termination of employment, and may also result in civil or criminal liability. All personnel are responsible for reporting any suspected violations of this policy.

Review and Revision:

This policy will be reviewed annually and updated as necessary to reflect changes in technology, legal requirements, and business needs.

X

Robert James
Managing Director

X

Richard James
Managing Director