McCorry®

MCCORRY USA CORP.

Cybersecurity Policy Statement

McCorry Group

McCorry Group is committed to safeguarding its information assets, customer data, and technology infrastructure against cybersecurity threats. Protecting the confidentiality, integrity, availability, and privacy of information is fundamental to maintaining stakeholder trust and supporting sustainable business operations.

Cybersecurity is integrated into our governance framework and operational processes to ensure responsible risk management and regulatory compliance.

Governance & Oversight

Cybersecurity oversight is embedded within executive management responsibilities. Our leadership team ensures that information security risks are identified, evaluated, and managed in alignment with business objectives.

·Cybersecurity risks are assessed regularly.
·Security controls are reviewed and updated to address evolving threats.
·Security considerations are incorporated into strategic planning and project development.

Risk Management Approach

We maintain a structured cybersecurity risk management program designed to:
·Identify potential threats and vulnerabilities.
·Assess risk based on likelihood and business impact.
·Implement appropriate technical and organizational safeguards.
·Monitor and continuously improve security controls.

Access Control & Identity Security

·Access to systems and sensitive information is restricted to authorized individuals based on business need.
·Role-based access principles are applied.
·Strong authentication mechanisms are enforced for critical systems.
·User access rights are reviewed periodically.
·Access is promptly removed upon role change or termination.
·Administrative and privileged activities are monitored to reduce the risk of unauthorized use.

www.mccorry.com
2475 Northwinds Parkway, Suite 200, Alpharetta
GA, 30009, U.S.A.

McCorry®

MCCORRY USA CORP.

Data Protection & Privacy

We apply appropriate safeguards to protect company and customer data throughout its lifecycle.

·Sensitive data is protected through encryption and secure transmission methods.
·Data retention practices are defined to meet legal and contractual requirements.
·Secure disposal procedures are followed when data is no longer required.
·Privacy obligations are considered in system design and operational processes.

Employee Awareness & Responsibility

·All personnel share responsibility for protecting information assets.
·Security awareness training is provided regularly.
·Employees are required to comply with confidentiality and acceptable use requirements.
·Security responsibilities are defined and communicated.

Third-Party & Supply Chain Security

·We recognize that cybersecurity extends beyond our organization.
·Vendors and service providers are evaluated for security practices prior to engagement.
·Third-party risks are reviewed periodically.

Monitoring & Continuous Improvement

·Our cybersecurity framework is designed for continuous improvement.
·Security events are monitored and investigated.
·Policies and procedures are reviewed periodically.
·Controls are enhanced as threats evolve and business needs change.

Our Commitment

McCorry Group is committed to maintaining a resilient cybersecurity posture that protects our stakeholders, supports operational continuity, and meets applicable regulatory and certification requirements.

We continually strengthen our cybersecurity capabilities to ensure responsible governance and long-term business sustainability.

For further information regarding our cybersecurity practices, please contact us.

www.mccorry.com
2475 Northwinds Parkway, Suite 200, Alpharetta
GA, 30009, U.S.A.