CWA ENTERPRISE Security Policy

Purpose and Scope This security policy outlines the measures that CWA ENTERPRISE will take to ensure the confidentiality, integrity, and availability of our information systems and data. This policy applies to all employees, contractors, and third-party vendors who have access to our systems and data.

# Access Control

Access to CWA ENTERPRISE information systems and data will be granted on a need-to-know basis. Access will be controlled with unique user IDs and strong passwords. Passwords must be changed every 90 days and must be at least 12 characters long, including a mix of upper- and lower-case letters, numbers, and special characters. Access to sensitive data will be further restricted using multi-factor authentication, where feasible.

# Traffic Management

CWA ENTERPRISE will implement traffic management measures to ensure that our network and systems are protected from unauthorized access, denial of service attacks, and other security threats. These measures include:

# Firewall

CWA ENTERPRISE will deploy a firewall to restrict access to our network and to prevent unauthorized access from external networks. The firewall will be configured to allow only authorized traffic to enter and exit our network.

# Intrusion Detection System (IDS)

CWA ENTERPRISE will deploy an IDS to detect and respond to potential security threats. The IDS will monitor network traffic for signs of suspicious activity, such as attempts to exploit vulnerabilities or access restricted resources.

# Virtual Private Network (VPN)

CWA ENTERPRISE will require employees, contractors, and third-party vendors who need remote access to our systems to use a VPN. The VPN will provide secure, encrypted communication over the internet, preventing unauthorized access to our network and data.

# Incident Response

CWA ENTERPRISE will implement an incident response plan to quickly and effectively respond to security incidents. The incident response plan will include procedures for identifying and containing security incidents, as well as procedures for reporting incidents to appropriate authorities and conducting post-incident analysis.

# Compliance

CWA ENTERPRISE will comply with all applicable laws, regulations, and industry standards related to information security. We will periodically review and update our security policy and related procedures to ensure ongoing compliance.

# Enforcement

Any CWA ENTERPRISE employee, contractor, or third-party vendor who violates this security policy may be subject to disciplinary action, up to and including termination of employment or contract. Violations may also be reported to appropriate law enforcement agencies.

By implementing these access control and traffic management measures, CWA ENTERPRISE can help ensure the security of our systems and data, protecting our organization and our stakeholders from potential harm.