ELEVION GROUP AUP

Information security is crucial at Elevion Group, with employees being the first line of defense. This policy outlines the acceptable use of Elevion Group's information systems to ensure the safety of company systems, data, and processes.
This policy applies to all Elevion Group entities, employees, third parties, vendors, and contractors who access Elevion Group's information systems, including business applications, servers, desktops, laptops, databases, network devices, mobile platforms, and cloud applications.

The key policy statements

- **End User Devices:** Systems must be used for authorized purposes only. Inappropriate or illegal use is prohibited. Confidentiality of information must be protected.
- **Portable Devices:** Protect devices from loss or theft. Use only media provided by Elevion Group for business use.
- **Mobile Devices:** Protect devices from loss and unauthorized access. Only approved applications should be installed.
- **Access Control:** Use and protect user credentials responsibly. Unauthorized access and bypassing security controls are prohibited.
- **Password Security:** Use strong, unique passwords and keep them confidential. Use of secure password managers is authorized.
- **Internet Usage:** Internet access is for work-related tasks. Accessing inappropriate or illegal content is prohibited.
- **Electronic Communications:** Use company systems for business purposes only. Personal communication technologies should not be used for company business.
- **Working from Home:** Ensure physical security of company equipment and prevent eavesdropping.
- **Privacy and Compliance:** Follow organizational policies for data privacy and intellectual property.
- **Cloud Computing:** Use only approved cloud services for business processes.
- **Social Media:** Use authorized accounts for company communication. Personal opinions should be clearly distinguished from company views.
- **Virus Protection:** Install anti-virus software on all devices. Be cautious with email attachments and downloads.
- **Software Usage:** Install only approved and licensed software. Use of online solutions requires authorization.
- **Security Incidents:** Report any suspected security incidents or weaknesses immediately.
- **Security Awareness:** Participate in regular security awareness training.
- **Clean Desk Policy:** Ensure sensitive information is not accessible when unattended. Lock screens and secure devices.