EP Power Europe

EPPE Group Cybersecurity Principles

EP Power Europe, a.s. ("EPPE") and the subsidiaries and companies controlled by it ("EPPE Group") are committed to conducting their business activities with a strong focus on protecting information, technology, and digital services to respond to continuously evolving IT environment complexity, new security threats and regulatory requirements.

This document defines the EPPE Group's key security principles as a guidance for the individual EPPE companies. They implement these principles in their own binding internal security policies, standards, and procedures that are appropriate to the purpose of each company, its concrete business functions, physical and IT environment, regulatory obligations. This information security management system is then updated whenever a significant change in the company's security risk situation occurs.

The EPPE Group follows these key cybersecurity principles:

A. **Organizational security governance.** Establish an effective security governance system to manage all security areas in your organization. The top management should be involved and provide necessary support.

B. **Risk assessment.** Define acceptable security risk levels in your organization by performing regular risk assessments.

C. **Security policies.** Implement, approve, and properly communicate information security policies to all employees and relevant external subjects. Update company information security policy and topic specific security policies to follow organizational changes and results of risk assessments.

D. **Security awareness.** Conduct regular mandatory employee training programs to improve user security awareness. Apply this obligation to relevant external entities accessing organization's internal information systems or treat this responsibility with them contractually.

E. **Asset Management**. Identify important assets in the company, manage their ownership, define appropriate protection level, and handle them accordingly.

F. **Identity management and Access control.** Implement identity management to enable automatic (de)provisioning of user accounts, password management, Single Sign-On (SSO) and Role-Based Access Control (RBAC) to achieve access governance. Establish access control processes and measures to limit users' access to information systems and restrict their authorized activities to a justified minimum required by the users' roles. Pay special attention to privileged users and shared accounts if they cannot be eliminated.

G. **Secure connectivity and Remote workplace.** Implement protection for end-user devices, mobile equipment, servers, and industrial control systems to securely connect to organizational IT

environment from internal network or remotely from external or public networks. Use preferably two-factor authentication for accessing internal network from outside.

H. **Malware protection.** Implement anti-malware scan solutions or analytical tools, filtering methods (e-mail, web, network). Define relevant processes and focus on building and testing of users' security attentiveness regarding phishing or similar attacks.

I. **Threat and vulnerabilities management.** Implement processes and depending on your situation also technical means for incidents' detection and preventive mitigation of actual threats or vulnerabilities.

J. **Monitoring and continuous risk evaluation**. Implement processes and technical means for monitoring information systems, industrial control systems, suspicious network activities and unusual user behavior. The effective continual/regular analysis of monitoring results is essential.

K. **Patch management and Secure configuration.** Create processes and inventories to ensure equipment are updated/patched and follow defined security configuration standards.

L. **Network security**. Protect your network by addressing security in the network architecture design, segregate network according technical, operational and risk domains, clearly define perimeter characteristics and access rules. Network connections to external networks, external partners, or remote access connections, should be directed through proxies/DMZs and filtered.

M. **Cyber resilience.** Establish processes for effective incident response according incident management plans and disaster recovery procedures. Nominate incident response staff. Conduct regular testing of your resilience by independent security reviews or penetration testing. Implement strong data protection & storage mechanisms to mitigate ransomware attacks to your data.

N. **Business continuity.** Create and verify business continuity plan to maintain business functions and essential IT services in adverse situations, e.g. during a crisis, disaster, severe IT attack or incident.

O. **Trusted supply chain.** Address security requirements in all contracts with external entities before granting access to sensitive organizational information assets and regularly evaluate the contract requirements and their fulfillment.

P. **Physical protection**. Protect all secure or operational critical areas by physical barriers such as walls, entry controls e.g. electronic controlled entry gates, screening, manned reception desks or locked racks/screens. Allow only authorized parties to enter internal offices under conditions and measures reflecting identified risk.

Q. **Industrial Control Systems (ICS)**. Implement specific security processes and measures for ICS environment, addressing complex, diverse nature of ICS and differences in comparison with conventional ICT world. Ensure relevant control system engineers, telecommunications specialists and other staff are notified of their assigned roles and responsibilities regarding information security aspects of ICS.

R. **Human resource security**. Establish appropriate process for all phases a) prior to employment (e.g. screening) b) during employment (e.g. management responsibility, cyber training, disciplinary process) c) termination and change of employment (covering what happens when people leave or change roles).

S. **Regulatory compliance.** Establish appropriate processes to achieve regulatory compliance especially in GDPR and local national NIS directive implementation (cyber security legislation).

T. **Security in IT and ICS lifecycle.** Incorporate cybersecurity in all life cycle phases of IT and ICS systems especially in procurement, operation, and change management.

EPPE Group companies follow as minimum these key group cybersecurity principles and are responsible for a selection and implementation of specific security measures to meet these principles. They should also look to leverage security knowledge and experience from other EPPE subsidiaries and companies wherever possible.

Approved by the EP Power Europe, a.s. Board of Directors on 9 April 2021