ATTACHMENT "B"

El Paso Electric	TECHNOLOGY & CYBERSECURITY		
		Date	12/5/2023
New Vendor Cybersecurity Questions		CONFIDENTIAL	

Purpose

This document lists the basic cybersecurity requirements EPE should be asking new possible vendors do describe and adhere to. As vendor evaluations and selections become clearer, Information Security may ask for more detailed questionnaires such as the SIG Lite or SOC II reports.

Scope

All new IT vendors.

Requirements

1. Vendor shall provide summary documentation of the product's security features and security-focused instructions
2. Does vendor have an Information Security Policy implemented across the organization which includes officer level approval?
3. Would they be able to share a SIG-Lite Questionnaire or SOC II report (if solution is hosted)?
4. Authentication and password management
    a. Active Directory Integration?
    b. SSO/Azure AD
    c. Support for Multi-Factor Authentication
5. Authorization and role management
    a. Must support role-based access
6. Audit logging and analysis
    a. Account activity must be logged
    b. Must have time stamps and control access to audit trails and log files
    c. Log export should be supported
7. Network, host and data security
    a. Data Storage Locations
        i. Provide detailed information on where our data will be stored when using your services. Do you have different geographical regions as an option?
        ii. What are the physical and digital security measures implemented at these data storage locations?
    b. Do you support Conditional Access?
    c. Firewalls
    d. If multi-tenet, will EPE be separate from other tenets?
    e. Multi-Factor?
        i. Is MFA authentication used for all remote administrative access including access to production environments?

   f. Do you support VPN connectivity?
   g. Types of end-point security (AV, Malware, EDR, etc.)
   h. IDS/IPS/HIDS
8. Patch Management and validation testing
   a. How are vulnerabilities found and patched?
   b. Is there a regular patch release schedule?
   c. Vendor needs to provide appropriate software and service updates and/or workarounds to mitigate all vulnerabilities
9. Cryptography and key management
   a. Encryption at rest
   b. Encryption in transit
      i. Must support TLS 1.2 and above
   c. If Hosted, is it Azure, AWS, Google?
10. Physical Security
   a. How does the vendor secure it's data centers, offices?
11. Data validation and sanitization
   a. Web Application Firewall support?
12. Third party component analysis
   a. What third-party components are required? (i.e. Java, .NET, Apache, etc.)
   b. Does the system depend on any legacy applications that are no longer supported? i.e. End-of-Life Windows or SQL/Oracle versions
13. Backup and Recovery
   a. Explain Data Retention/Archival policies
   b. Ransomware protection

Additional Documentation

Not Applicable

Review and Revision History

Date	Version	Revised By	History
6/8/2021	1.0	E. Bernal	Document Creation
9/3/2021	1.1	E. Bernal	Added question on legacy application dependency
12/5/2023	1.2	E. Bernal	Added new questions