SCHEDULE A: Standard Cyber Security Requirements for Vendors

These standard cyber security requirements (**"Cyber Requirements"**) apply to all vendors, subcontractors, agents, suppliers, and any other independent contractors (**"Vendor"**) supplying goods or performing services (collectively **"Services"**) for any member of the Ledcor Group of Companies (**"Ledcor"**) under an agreement between the parties ("**Agreement**"). The Cyber Requirements shall be deemed the minimum requirements the Vendor is required to meet. Where such Services are performed as a subcontractor to Ledcor under an agreement with a customer, client, or project owner (**"Client"**), if the terms of the agreement with the Client contain similar cyber security requirements, the Vendor shall meet the more stringent requirements.

1. General Statement on Cyber Security

The Vendor acknowledges the importance of cyber security and is committed to operating in a secure way, protecting its own and Ledcor's data and systems. The Vendor's cyber security program (the "**Cyber Security Program**") must have the necessary organizational support and resources and must contain administrative, technical, and physical safeguards compliant with applicable laws and consistent with reasonable cyber security practices as stipulated in the National Institute of Standards and Technology's Cybersecurity Framework ("**NIST CSF**"), ISO/IEC 27000, or similar frameworks. The Cyber Security Program shall be continually improved in alignment with changing regulatory requirements, threats and risks, and cyber security practices.

2. Operational Security

Consistent with reasonable cyber security practices as stipulated in the NIST CSF, ISO/IEC 27000, or similar frameworks, the Vendor shall maintain operational security safeguards, to protect systems and data, and to reduce the likelihood and impact of cyber incidents and breaches including, without limitation, the following:

a. Password Management: Vendor shall maintain password and account management practices which include:
    i. Encrypting passwords using reasonable practices and techniques.
    ii. Using multi-factor authentication.
    iii. Enforcing reasonable password complexity controls.
    iv. Limiting failed attempts before account lockout.
    v. Not allowing cleartext passwords.
    vi. Ensuring that password reset processes do not send credentials; and
    vii. Maintaining logs of user authentication, password changes and other account management related activities.

b. Identity and Access Management: Vendor shall maintain processes for identity and access management, including ensuring identities are disabled and access revoked within a reasonable time, upon termination, or when access is no longer needed. When accessing Ledcor and Client systems, Vendor shall follow, where applicable:
    i. Ledcor processes for requesting access to Ledcor systems and networks, as required to perform their role.
    ii. Client processes for requesting access to Client systems and networks, as required to perform their role.

c. Malware Protection: Vendor shall maintain up-to-date malware software detection systems on all devices used for Ledcor contracts, ensuring that malware software detection systems are configured to:
    i. Log all malware detection activities.
    ii. Delete infected files that cannot be repaired.
    iii. Update malware detection system signature files (at a minimum daily) for devices used for Ledcor contracts.
    iv. Automatically scan removable media.
d. Vulnerability and Patch Management: Vendor shall maintain processes to ensure that all devices used for Ledcor contracts are fully patched, prior to performing any work for Ledcor, or Client, and shall maintain a regular patch schedule, using a risk-based approach.
e. Network Security: Vendor shall maintain reasonable network security controls to protect applications, computing system devices and data from cyber threats.
f. Backup and Recovery: Vendor shall maintain backup processes, procedures, and associated infrastructure for systems used in the delivery of services for Ledcor including, without limitation, the following:
    i. System software, application software, and data shall be securely backed-up on a reasonable schedule.
    ii. Procedures for recovering system software, application software, and data shall be documented and periodically tested.
g. Data Security: Vendor shall maintain reasonable data security protection controls to protect Ledcor's and Client's data when accessing, storing, and transmitting such data.
h. Logging & Monitoring: Vendor shall ensure that event logs recording appropriate user activities, exceptions, faults, and Cyber security events are maintained and are regularly reviewed. Logging facilities and log information shall be protected against tampering and unauthorized access.
i. Change Management: Vendor shall maintain information systems change management processes to ensure that changes to systems, associated processes, and facilities are controlled. Where Vendor provides Services involving Ledcor or Client systems, Vendor shall follow the applicable Ledcor or Client change management processes.
j. End User Devices: When using non-Ledcor managed or configured devices at Ledcor Client sites, Vendor shall ensure that device(s) used in the delivery of Services are securely configured with reasonable cyber security controls, as stipulated in NIST Special Publication 800-53, Center for Internet Security benchmarks or similar standards.
k. Cyber Security Incident Response: Vendor shall maintain a cyber security incident response program, including a response plan, to reasonably detect, respond, and recover from cyber security incidents and breaches.
l. Return of Assets: Vendor shall return all Ledcor and Client issued devices upon completion or termination of the Agreement.

3. Notification of Cyber Incident or Breach

In the event of a cyber security incident or breach resulting in suspected or actual loss of Ledcor data or unauthorized access to any system containing or having direct access to Ledcor data, the Vendor shall:

a. Immediately notify Ledcor of the breach, in writing within 48 hours of becoming aware of a cyber incident/breach.

b. Promptly conduct a forensics examination to determine to what extent such information was compromised.
c. Promptly provide, in writing, details concerning the incident/breach.
d. Promptly cooperate with Ledcor, any affected Client, regulators, and law enforcement.
e. Promptly take measures to restore and enhance its Cyber Security Program to avoid further incidents/breaches.

4. Use of Subcontractors

a. The Vendor shall require all subcontractors performing any portion of the Services to meet all the Cyber Requirements.

5. Data Residency / Offshore Restrictions, Ownership and Return of Data

a. Data Residency/Offshore Restrictions: Vendor shall not store, transmit, or process Ledcor data outside of the United States or Canada without prior written consent from Ledcor.
b. Data Ownership: All Ledcor data, regardless of where it is transmitted, processed, or stored, and regardless of whether such data is maintained on magnetic tape, magnetic disk, or any other storage or processing device, including any data derived from it, remains the sole and exclusive property of Ledcor, retaining all right, title, and interest, whether express or implied. The Vendor has no and acquires no right, title, or interest, whether express or implied, and will only use Ledcor's data for the purposes set forth in the Agreement.

6. Training

Where applicable, the Vendor shall complete all Ledcor and Client cyber related training required or assigned, prior to the commencement of any Services in accordance with the Agreement.

7. Compliance with Ledcor Cyber Requirements

a. Vendor shall:
   i. Comply with applicable laws and regulations in its use of Ledcor's data and systems, including, without limitation using ONLY Ledcor and Client authorized applications to execute the Services, NOT storing Ledcor and Client data locally on Vendor devices or on removeable media, and NOT circumventing cyber security controls on Ledcor and Client systems or applications used in the delivery of Services.
   ii. Comply with applicable privacy laws and regulations, in its use of Ledcor data and systems.
   iii. Comply with other applicable Ledcor cyber security processes and procedures, as directed by Ledcor.
   iv. Fully cooperate with Ledcor's periodic security reviews to validate compliance with the Cyber Requirements.
b. The Vendor will maintain a compliance process to ensure the Cyber Security Program is meeting the Cyber Requirements as well as all applicable legal and regulatory requirements.