Honeywell

Security Obligations for Confidential Information Exhibit

This Security Obligations for Confidential Information Exhibit is incorporated into the Non-Disclosure Agreement ("NDA") between Honeywell and Company or Supplier, as applicable. If there is a conflict between the provisions of this Security Exhibit, the NDA, or any other written instrument between the Parties, the stronger control statement will supersede the weaker control statement. The Party receiving Confidential Information (the "Recipient"), which may be Honeywell, Customer, or Supplier, as specified in the NDA, will maintain at least the following physical, administrative, and technical security controls to protect Confidential Information under its care, custody, or control:

1. **Physical Controls:**
   a. Control physical access to all facilities and information processing areas with Confidential Information to ensure only authorized persons with unique, identifiable authorization credentials are permitted access to such facilities;
   b. Monitor physical access to facilities to detect and respond to physical security incidents; and
   c. Employ appropriate access control mechanisms to control and validate authorization of visitors' access to facilities before granting access.

2. **Technical Controls:**
   a. Implement industry-standard technical measures, including formal access management process in accordance with principles of "least privilege" and "need to know";
   b. Require and enforce password complexity requirements with minimum of eight (8) alphanumeric characters of mixed case;
   c. Prevent reuse of password for at least one year or maintain password history of 14 or more passwords remembered;
   d. Configure accounts to be locked out after five (5) consecutive unsuccessful login attempts;
   e. Terminate idle sessions after a maximum of two (2) hours of inactivity;
   f. Employ encryption and strong authentication mechanisms including multifactor authentication for privileged access, and remote access;
   g. Encrypt (using industry-standard protocols) Confidential Information and authentication credentials in transit at all times;
   h. Encrypt Confidential Information when on mobile media or storage devices;
   i. Encrypt all sensitive or highly Confidential Information (e.g., trade secrets, intellectual property) at rest at all times.
   j. Maintain whole disk encryption for any mobile devices containing Confidential Information;
   k. Employ protection mechanisms to detect and eradicate malicious code at relevant access points;
   l. Scan network environment for vulnerabilities periodically (on a quarterly basis or more frequently) and conduct penetration testing at least annually and promptly remediate any identified vulnerabilities;
   m. Maintain enterprise patch management process to identify and deploy patches and system updates to assets accessing or managing Confidential Information;
   n. Install security-relevant software and firmware updates in accordance with vendor recommendations;
   o. Monitor network and key applications to detect cyber-attacks or indicators of potential attacks;
   p. Use automated processes and tools, including intrusion detection & prevention, to support real-time analysis of networks;
   q. Where any U.S. Government information is in scope, adhere to applicable requirements such as NIST SP 800-171;
   r. Maintain incident response program in compliance with industry standards and notify Party within 24 hours for incidents involving Party's Confidential Information; and
   s. Where software is provided, ensure all products are developed following secure software development practices including static and dynamic application security testing for each version release.

3. **Administrative Controls**
   a. Perform, in accordance with applicable laws and regulations, background check screening (including, where not prohibited by law, identity verification and criminal history) on personnel prior to authorizing access to Confidential Information;
   b. Train personnel on information security awareness within 30 days of onboarding or prior to gaining access to Confidential Information, and annually thereafter; and
   c. Revoke physical and cyber access rights and mechanisms (e.g., keys or access cards) provided to personnel upon within one (1) business day of employment termination.