Honeywell Security Obligations For Suppliers Exhibit

The Honeywell Security Obligations For Suppliers Exhibit ("Security Exhibit") forms part of the Purchase Order ("PO") between Honeywell and Supplier. If there is a conflict between the provisions of this Security Exhibit or the PO that references this Security Exhibit, this Security Exhibit shall prevail. Supplier will maintain at least the following physical, administrative, and technical security controls to protect Honeywell 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 any facilities having access to Confidential Information;
   b. Issue authorization credentials for facility access to uniquely identify every individual that has physical access to facilities;
   c. Monitor physical access to facilities to detect and respond to physical security incidents; and
   d. Employ appropriate access control mechanisms to control visitors' access to facilities and validate approval of visitors before granting access to facilities.
2. **Technical Controls:**
   a. Implement industry-standard technical measures, including a formal access management process in accordance with the principles of "least privilege" and "need to know";
   b. Configure information management systems to disable/delete inactive personnel accounts after 90 days and end user or customer accounts after 365 days;
   c. Require and enforce password complexity requirements with minimum of eight (8) alphanumeric characters of mixed case and prevent reuse of a password for at least one year;
   d. Enforce 90-day expiration for single-factor and 365-day expiration for multifactor authentication;
   e. Configure accounts to be locked out after five (5) consecutive unsuccessful login attempts and terminate idle sessions after fifteen (15) minutes for any sessions;
   f. Employ encryption and strong authentication mechanisms such as hardware token-based authentication and multifactor authentication (as applicable) for privileged access, wireless access, and remote access;
   g. Encrypt (using industry-standard protocols) Confidential Information and authentication credentials in transit over public and/or wireless networks and when on mobile media or storage devices;
   h. Encrypt all sensitive or highly Confidential Information (e.g. trade secrets, IP in development) at rest;
   i. Maintain whole disk encryption for any mobile devices containing Confidential Information;
   j. Employ protection mechanisms to detect and eradicate malicious code at relevant access points;
   k. Scan its environment for vulnerabilities periodically (on a quarterly basis or more frequently) and conduct penetration testing at least annually, and promptly remediate any identified vulnerabilities;
   l. Maintain an enterprise patch management process to identify and deploy patches and system updates to any asset with Confidential Information;
   m. Install security-relevant software and firmware updates in accordance with vendor recommendations as soon as possible;
   n. Monitor the network and key applications, at a minimum, to detect cyber-attacks or indicators of potential attacks or unauthorized or unapproved network services;
   o. Use automated processes and tools, including intrusion detection & prevention, to support real-time analysis of networks;
   p. Maintain an incident response program in compliance with industry standards (e.g., ISO/IEC 30111, ISO/IEC 29147) and notify Honeywell within 24 hours for incidents involving Confidential Information;
   q. To the extent software is provided, ensure that all products are developed following secure software development industry best practices, and regularly perform quality and cybersecurity reviews and testing of products;
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 Confidential Information;
   b. Train all personnel on information security awareness within 30 days of onboarding or prior to gaining access to Confidential Information, and annually thereafter;
   c. Revoke physical and cyber access rights and mechanisms (e.g. keys or access cards) provided to personnel upon termination as soon as possible (not to exceed one business day);
   d. 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;
   e. Train all personnel on information security awareness within 30 days of onboarding or prior to gaining access to Confidential Information, and annually thereafter;
   f. Revoke physical and cyber access rights and mechanisms (e.g. keys or access cards) provided to personnel upon termination as soon as possible (not to exceed one business day); and
   g. Upon Honeywell's request, provide sufficient evidence and documentation to demonstrate compliance with Supplier's obligations hereunder.