WPS VENDOR PERSONNEL SECURITY REQUIREMENTS

SECTION 1 – ALL WPS AREAS.

A. All Vendor personnel ("Contractors") who require **unmonitored access to WPS systems** must: satisfactorily complete a background check that meets the requirements identified by WPS for the Contractor's role. Prior to starting work, Vendor shall submit the WPS Background Check Attestation confirming that Vendor has completed the required background check for each Contractor accessing WPS' systems. Vendor may rely on an existing background check if it meets WPS' requirements and was conducted within the last 5 years. Vendor must retain background check results for 3 years after the completion of the Contractor's assignment at WPS.

In addition, Contractors shall (a) notify WPS in writing of new felony convictions within thirty (30) days of conviction, (b) sign the WPS Non-Employee Confidentiality Agreement every 365 days, (c) abide by all applicable WPS privacy and security policies, training and procedures provided by WPS, (d) follow the WPS Facility Rules for Visitors while on WPS premises, (e) complete and sign a Conflict of Interest Questionnaire every 365 days, and (f) complete HIPAA Privacy, WPS Code of Conduct, and Records Retention training at the beginning of the Contractor's assignment to WPS and refresher training at least once every 365 days thereafter.

A Contractor is not eligible for assignment at WPS if (a) convicted of a felony in the prior 7 years substantially related to the Contractor's role, (b) listed in a sex offender registry database and the conviction is substantially related to the Contractor's role, or (c) named on the U.S. Department of Health & Human Services Office of Inspector General (OIG) List of Excluded Individuals and Entities, the Office of Foreign Assets Control (OFAC) Specially Designated Nationals List, or the System for Award Management (SAM) excluded parties list. Professional references and education verification are also required as part of the background check.

B. Contractors who require **unescorted access to WPS premises** but no unmonitored access to WPS systems must (a) sign the WPS Non-Employee Confidentiality Agreement every 365 days, (b) abide by all applicable personnel, privacy and security policies, training and procedures provided by WPS, and (c) follow the WPS Facility Rules for Visitors while on WPS premises. Vendor must complete and submit the WPS Attestation for Contractors with No Systems Access and, upon request, provide documentation to WPS showing that such Contractors have undergone a full background check within the last 5 years. A Contractor will not be eligible for assignment at WPS if (a) convicted of a felony in the prior 7 years that is substantially related to the Contractor's role, (b) listed in a sex offender registry database and the conviction is substantially related to the Contractor's role, or (c) named on an OIG, OFAC, or SAM excluded parties list. Vendor must retain background check results for 3 years after the completion of the Contractor's assignment at WPS.

C. Vendor must notify WPS as soon as reasonably practicable, but no later than 72 hours after it becomes aware that a Contractor with **unmonitored access to WPS systems or unescorted access to WPS premises is** no longer employed by or contracted with Vendor, is on a leave of absence, or will no longer be performing services for WPS.

D. Contractors who require **monitored access to WPS systems** (e.g., screen share with WPS employee) may also be subject to background checks and personnel security requirements.

SECTION 2 – ADDITIONAL COMMERCIAL HEALTH INSURANCE REQUIREMENTS. Contractors performing services that support WPS's Health Plan Division, including Contractors in IT roles, are not eligible for assignment at WPS if they have ever been convicted of a felony involving dishonesty or breach of trust.

SECTION 3 – ADDITIONAL MEDICARE REQUIREMENTS. Contractors performing services that require access to or use of systems storing or processing Centers for Medicare and Medicaid Services (CMS) data must: (a) complete Medicare Security Training, (b) only access CMS data on U.S. soil, and (c) have lived in the United States for at least three of the last five years. Additionally, Contractors performing services that involve Medicare program funds, directly or indirectly, must also undergo a credit check and employment verification.

SECTION 4 – ADDITIONAL TRICARE REQUIREMENTS. Contractors performing services that: (i) require physical and logical access to an unclassified DoD or a CAC-enabled unclassified network shall have completed a favorable and adjudicated Tier 1 background investigation or (former) National Agency Check with Inquiries (NACI) or equivalent; and (ii) require access via a WPS system to data protected by either the Privacy Act of 1974, as amended, or the HHS HIPAA Privacy and Security Final Rule shall have completed background checks that: (a) verify U.S. citizenship; (b) verify education (degrees and certifications) required for the position; (c) screen for negative criminal history at all levels (federal, state, and local); and (d) screen for egregious financial history.

SECTION 5 – ADDITIONAL VETERANS AFFAIRS REQUIREMENTS. Contractors performing services that require access to or use of Veterans Affairs (VA) data or systems must undergo employment verification.