# ATTACHMENT X: SECURITY REQUIREMENTS FOR VENDOR STAFF AND CONTRACTORS

****

**Security Requirements for Vendor Staff and Contractors**

All Vendor provided and Contract Staff (e.g. seasonal temps) must fulfill required security checks prior to beginning work at NCDOR. Required security checks vary based on system and information access level, and generally follow the principle of least privilege. Attachment 1.A – Vendor and Contractor Security Requirements Matrix provides a guide for the most common levels of access and the corresponding security requirements for each level. NCDOR IT Security will advise and approve access levels not represented on Attachment 1.A.

Required documentation must be submitted prior to beginning work at NCDOR. The documentation should be submitted as determined by the NCDOR Contract Manager.

Guidelines include the following:

* Attachment 1.A – Vendor and Contractor Security Requirements Matrix
* IT Security review and approval if special access is required
* As defined in the Requirements Definitions below

Requirements Definitions:

1. **Nondisclosure Agreement:** Any staff performing any work under this contract must sign a NCDOR non-disclosure agreement (NDA) agreeing to maintain the confidentiality of any NCDOR data to which the Vendor Staff and/or Contractor may have access.
2. **Criminal Background Checks:** Applicable staff must submit to and successfully pass a criminal background check to be conducted by NCDOR for anyone who will be receiving or who will have access to NCDOR Data. These checks will be repeated every 5 years. It does not matter if the access is to paper or electronic NCDOR Data. NCDOR determines the conditions for passing background checks.
3. **Fingerprinting:** Completion of Federal Bureau of Investigation (FBI) fingerprinting, which is conducted to identify possible suitability issues, is required. These checks will be repeated every 5 years. Suitability issues are determined by NCDOR.
4. **Security Awareness Training:** NCDOR Security Awareness Training (DORSAT) is required annually. In order to receive NCDOR training, a valid business email is required for each person who is in scope and who is performing work for this contract on behalf of the Vendor and/or Contractor.
5. **I.T. Role-Based Security Training:** The Vendor and/or Contractor, for all applicable staff, provides annual I.T. role-based security training. Compliance with this requirement will be audited by NCDOR at random for compliance. I.T. role-based security training details and role scope can be found in the NCDOR Security Policy Manual - Control AT-3.
6. **A copy of NCDOR’s Security Policy Manual can be found at the following link:**

<https://www.ncdor.gov/documents/dor-security-policy-manual>

Attachment 1.A – Vendor and Contractor Security Requirements Matrix

**NOTE: Read all indicated footnotes carefully as these contain important information**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Level of Access | NDA | NCDOR Policy Manual Provided | \*Background Check | Security Awareness Training | \*\*Role-Based Training |
| 1Escorted access – Must Be Escorted at All Times | YES | YES | NO | NO | NO |
| Physical Access – Non-Escorted (Badge Access) | YES | YES | YES | YES | YES |
| 2Logical Access to NCDOR Data/Systems/Information (Has an Account) | YES | YES | YES | YES | YES |
| 3Logical Access to NCDOR Data/Systems/Information (Does Not Have an Account) | YES | YES | NO | NO | NO |
| 4Offsite Contractor Staff with Physical Access to NCDOR Data/Systems/Information | YES | YES | YES | YES | YES |
| Access to Unencrypted Paper or Electronic NCDOR Data | YES | YES | YES | YES | YES |
| 5Logical Access to Encrypted Data | YES | YES | NO | NO | NO |

\* Background check requirements include FBI fingerprinting and criminal background checks. For a full list of requirements, please refer to the NCDOR Security Policy Manual

\*\* Role-Based Training (RBT) is provided by Vendors and/or Contractors. Role scope is defined in the NCDOR Security Policy Manual > AT-3 Role-Based Training > Scope

1. Individuals may utilize NCDOR equipment as long as they will be supervised with the equipment at all times. Unsupervised access to equipment requires a unique account that ties back to the individual and all account requirements listed in this matrix are required.

2. Accounts must be unique and must tie back to the individual.

3. Applies to individuals that will potentially view NCDOR data on screens as part of logical maintenance of systems, but who do not have an account. Data cannot be sent outside of the Agency without NCDOR management approval of the data sent and NCDOR IT Security approval of the method used to send the data. Maintenance activities (including remote maintenance) must be supervised by badged NCDOR staff or by a badged NCDOR management-approved designee. Any systems used to facilitate remote supervision must be secure and approved by NCDOR IT Security.

4. Access to data is defined for these purposes as individuals that have access through the first barrier of the two-barrier rule. See IRS Publication 1075 – Minimum Protections Standards for more information.

5. Encryption methods must be FIPS 140-2 compliant.