UNIVERSITY OF CALIFORNIA
Agriculture and Natural Resources

Cybersecurity Expectations for Contractors & Contingent Workers

At University of California – Agriculture and Natural Resources (UC ANR), we prioritize the security of our systems and data. As a contractor/contingent worker, you are expected to adhere to ANR's cybersecurity policies and procedures to ensure the protection of sensitive information. The following expectations outline the minimum requirements for cybersecurity practices.

1. Access Control

- **Authentication and Authorization**: Contractors and Contingent Workers must use strong, unique passwords and multi-factor authentication where applicable. Access to systems and data must be restricted to authorized personnel only.
- **Least Privilege Principle**: Access should be granted based on the minimum necessary privileges to perform your job responsibilities. If the minimum access level includes capabilities beyond the scope of services, those additional capabilities should not be used or acted upon.
- **Personal Credentials**: Contractors and Contingent Workers must use their own credentials and never share login information with others.

2. Data Protection

- **Encryption**: All sensitive data must be encrypted both in transit and at rest using industry-standard encryption protocols.
- **Data Handling**: Contractors and Contingent Workers must ensure proper handling, storage, and disposal of data according to UC ANR's data protection policies.
- **Device Security**: Devices used to access UC ANR systems must have hard drive encryption, updated Endpoint Detection and Response (EDR) software, and the latest security patches. Contractors and Contingent Workers are not permitted to connect to UC ANR systems using personal devices. If a contractor and contingent worker only has a personal device, UC ANR will provide a secure device for accessing UC ANR's data. This device must be returned to UC ANR upon termination of the contract, completion of the project, or offboarding of the contractor or contingent worker.

3. Network Security

- **Secure Connections**: Use secure, encrypted connections (e.g., UC ANR VPN or Secure Tunnel) when accessing UC ANR networks remotely.

4. Incident Response

- **Reporting**: Immediately report any suspected or confirmed security incidents, breaches, or vulnerabilities to UC ANR's IT team.
- **Containment and Mitigation**: Follow UC ANR's incident response procedures to contain and mitigate any security incidents.

5. Compliance and Training

- **Regulatory Compliance**: Adhere to all relevant laws, regulations, and UC ANR policies regarding data security and privacy.

7. Contractor/Contingent Worker Employee Offboarding

- **Notification**:
  - **Contractors**: Notify UC ANR immediately when an employee exits your contracting company to ensure their access is revoked quickly.
  - **Contingent Workers**: Notify UC ANR IT immediately when an contingent worker exits to ensure their access is revoked quickly.
- **Access Revocation**: Ensure that access to UC ANR systems is revoked promptly for departing contractors/contingent workers.
- **Data Deletion:**
  - Contractors: After offboarding, any UC information/data used as part of the project must be provided to UC ANR for archival purposes and then deleted from the vendor/contractor's systems.
  - **Contingent Workers**: At separation, any UC ANR equipment used by the contingent worker must be returned to UC ANR.

By adhering to these cybersecurity expectations, contractors/contingent workers play a vital role in safeguarding UC ANR's information and systems. Failure to comply with these requirements may result in termination of the contract/contingent employment and potential legal action.

For any questions or further information, please contact UC ANR's IT team at help@ucanr.edu.