UTIA INSTITUTE OF AGRICULTURE
THE UNIVERSITY OF TENNESSEE

# UTIA Security Checklist for Outsourced Vendors

**Please provide a Yes, No, or N/A to each question. If a question is answered with a No or N/A, please provide additional information in the Comments section.**

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| 1. Does your organization have a documented and provable internal information security policy in place that details your information protection program for both logical and physical security? | | | | |
| 2. Is this policy reviewed and updated on a regular basis? | | | | |
| 3. May a copy of your information protection program be reviewed by UTIA ITS? | | | | |
| 4. In order to protect the confidentiality, integrity, and availability of UTIA sensitive data, does your organization ensure that: | | | | |
| a. Information and services are provided only to those authorized? | | | | |
| b. Information is protected so that it is not altered maliciously or accidentally? | | | | |
| c. Information and services are provided in conjunction with the vendor's disaster recovery and business continuity planning policy? | | | | |

| | | | | |
|---|---|---|---|---|
| 5. Is there a redundant site in another location your organization utilizes in the event of a disaster/failure? | | | | |
| 6. Are backup/recovery procedures updated and tested at least annually? | | | | |
| 7. What type of testing do you conduct for your business continuity and disaster recovery plan (i.e. simulation drills, walk-through exercises, tabletop exercises, actual drills, etc.)? | | | | |
| 8. How long do you estimate it will take to restore a product or service should you experience a serious business interruption that lasts more than one business day? | | | | |
| 9. Is access to offline media and backup data restricted to authorized individuals only? | | | | |
| 10. Are physical security measures in place to protect UTIA data from modification, disclosure, and destruction? | | | | |
| 11. Are servers protected by environmental controls? | | | | |
| 12. Are all visitors required to sign a security log and be accompanied by an escort while in the production area? | | | | |
| 13. Does your organization have an Information Security Administrator function separate from the System Administrator function? | | | | |

| | | | | |
|---|---|---|---|---|
| 14. Are external audits performed to test physical and information security controls? If so, how often are they performed? | | | | |
| 15. When was the last audit performed? | | | | |
| 16. Can a copy of your most recent external audit report be provided to UTIA for review? | | | | |
| 17. Do you log unauthorized login attempts to the system and application? | | | | |
| 18. Do you preserve event logs in case of a breach or investigation? | | | | |
| 19. Are logs kept in a central location, separate form the system components? | | | | |
| 20. How long are the logs retained? | | | | |
| 21. Does you organization use an intrusion prevention system (IPS)? | | | | |
| 22. Does you organization use an intrusion detection system (IDS)? | | | | |

| | | | | |
|---|---|---|---|---|
| 23. Are procedures in place for reporting and responding to possible security incidents? | | | | |
| 24. Do you have a separate development environment from your production environment? | | | | |
| 25. Is there a separate test environment? | | | | |
| 26. Are documented change control procedures in place? | | | | |
| 27. Are logical security measures in place to protect UTIA data from modification, disclosure, and destruction? | | | | |
| 28. Will UTIA data be securely segregated from the data of other customers? | | | | |
| 29. Will encryption be used on any UTIA data? If YES, please indicate the encryption to be used and where in the Comments filed. | | | | |
| 30. Who will have access to UTIA data? | | | | |
| 31. When are they authorized to handle/view UTIA data? | | | | |

| | | | | |
|---|---|---|---|---|
| 32. Who will handle the administration of the users in the application? | | | | |
| a. UTIA | | | | |
| b. Vendor | | | | |
| 33. Does your organization enforce a strong password policy? | | | | |
| 34. Are your employees/contractors required to sign a confidentially agreement? | | | | |
| 35. Do you have a mandatory security awareness program in place for employees to make them aware of confidential information, the company's security policies, standards, and good security practices? | | | | |

| | |
|---|---|
| Vendor: | |
| Completed By: | |
| Title: | |
| Date: | |
| Contact Information: | |