

A Sample Telework Security Checklist

Consider the following questions as appropriate, and use them to structure your teleworking security policy. These approaches, principles, and ideas are options to assist your organization in establishing plans for dealing with information security:



1. Do you have a remote access security policy?
2. Will you conduct regular reviews and revision of security policy to reflect technology changes, outdated approaches, or new product or service offerings affecting company/customer relationships and system interaction?
3. Does the remote access policy specify guidelines for the selection and implementation mechanisms that control access between authorized users and corporate computer and networks?
4. Does the remote access policy conform to all existing corporate communications guidelines?
5. Does the remote access policy address the physical protection of the communications medium, devices, computers, and data storage at the remote site?
6. Does the security policy require the classification of the functions, applications and data to determine the levels of security needed to protect the asset?
7. Does a policy exist to obtain access to important proprietary information at remote sites?
8. Does a policy exist that defines who is responsible in case of theft of hardware, software, or data at remote sites?
9. Does a policy exist for reporting unauthorized activity?
10. Does a policy exist for "appropriate" personal use of company equipment or family member use of company equipment?
11. Is there a policy on use of a PDA and company or confidential information maintained on the PDA?
12. Is there a policy outlining "appropriate" loading of non-company software?
13. Do remote access users have to sign a form stating they know and understand the remote access policies?
14. Is there an adequate backup plan for company data on the teleworker's local hard drive?
15. Is there a formal, complete, and tested disaster recovery plan in place for the remote sites?

Identification and Authorization

16. Do the remote access security controls require that users be identified before the requested actions are initiated?
17. Does each user have a unique identifier (user ID) and password?
18. Does the corporate site maintain and use authentication data for verifying the identity of a user?
19. Can the security controls uniquely identify each remote access user, device, and port?
20. Are there automatic time-out or lock-screen capabilities on the remote site equipment to control access during periods of non-use?

Access Control

21. Do the remote access security controls limit the unauthorized sharing of users' access rights?
22. Does the access control mechanism support the customizing of privileges for each user ID at remote sites?
23. Do the remote access security controls protect audit records from unauthorized access?
24. Are users provided with last login session information?
25. Are banners displayed regarding unauthorized usage?
26. Are banners displayed regarding the usage of monitoring policy?
27. Are there controls to prevent the uploading of unauthorized programs (e.g., virus programs) from remote site equipment to the corporate site?
28. Does the remote site have the capability to encrypt transmitted sensitive information, including authentication information?
29. Are users allowed only one remote connection to the corporate network (per user ID or address)?

Auditing

30. Does the remote access security mechanism record alarms and authentication violations as a default?
31. Does the audit record for each recorded event identify:
 - date and time of the event?
 - user or entity?

- origin of the event (e.g., network address, originating phone number)?
 - type of event?
 - success or failure of the event?
32. Is the audit trail information retained long enough to support reviews and analyses by security personnel and to meet corporate policy?
33. If dial-up access to the remote site is possible, does the audit mechanism record the details associated with each user access?
34. Can the security controls uniquely identify each remote access user, device, and port?

Integrity

35. Are virus-scanning capabilities required on remote sites? How often are they updated? What is the expectation for the teleworker to run the software?
36. Is personal firewall software installed on the teleworker's PC or laptop? How frequently is it updated?
37. Is access to public bulletin boards allowed?
38. Are there capabilities to perform network and server congestion management in terms of monitoring, detection, and enforcement functions?
39. Are measures in place to ensure the proper disposal of confidential data (paper, fax, digital, etc.) at remote sites?

Physical Security

40. Are the remote sites in physically secure locations?
41. If equipment is stolen, can the perpetrator access proprietary information?
42. Is a full physical inventory of remote site equipment and user systems maintained and periodically verified?
43. Are backup tapes and media available and secured on-site for remote site equipment?
44. Does a policy exist addressing fire, smoke, water, and hazardous material contamination damage at a remote site?
45. Is all paper data (proprietary, confidential, etc.) physically secure at the remote site?
46. Is all computer data (floppies, hard drives, etc.) physically secure at the remote site?
47. Is all media destruction (proprietary, confidential, etc.) at the remote site consistent with corporate security policies?

48. Is there a process for return of equipment and proprietary data upon termination of employment?
49. Does a policy exist for repair of equipment that contains proprietary information?
50. Is there insurance for liability and personal injury at the remote site?

Security Administration

51. Are organizational responsibilities for remote access security defined?
52. Is there a remote access security administrator?
53. Is security a part of the defined responsibilities for the personnel who monitor, maintain and control various remote site equipment?
54. Is there a process for authorizing new remote users, authorizing and updating remote user access capabilities, and deleting access when no longer needed?
55. Are there periodic reviews of remote user privileges to ensure that capabilities remain commensurate with job functions?
56. Do security event triggers generate alarms to provide administrator notification?
57. Are security alarms properly categorized in terms of severity? Can the administrator modify triggers?
58. Do the remote access security controls permit only authorized users (administrators) to grant access privileges to remote site equipment for new, authorized users?
59. Do the remote access security controls allow network devices to be isolated when there is a compromise?
60. Are there defined administrator responsibilities to isolate a compromised device?
61. Do the remote access security controls include testing, detecting and reporting communication errors (e.g., high re-transmission rate)?
62. Is there a way to prevent bypass of the audit and alarm mechanisms by resetting remote access devices to invoke an insecure default configuration?
63. Is periodic testing for unauthorized access, denial of service, or other security weaknesses performed?
64. Is there a defined practice of reviewing audit information on a periodic basis?
65. Are there reporting capabilities to provide information on user profiles and access rules?
66. Are there adequate controls to restrict access to and use of network troubleshooting equipment (e.g., protocol analyzer)?
67. Are there adequate controls to restrict access to and the use of network management software tools?

- 68. Is there a capability to force re-authentication after the server has been unavailable?
- 69. Is there a capability to force sign-off and prevent sign-on during system maintenance?
- 70. Are there means to run scheduled unattended backups of the remote site equipment?
- 71. Are all security functions and software changes made only by an authorized administrator?
- 72. Is there a way to ensure that only authorized, legally acquired software (e.g., applications, tools) are installed and used on remote-site equipment?
- 73. Are backup copies of authorized software and documentation available?
- 74. Are purchasing records and other proof of licensing requirements for software properly maintained?

Architecture and Topology

- 75. Is network equipment in place to separate traffic according to user communities?
- 76. Is the remote access equipment interconnected with less trusted or untrusted (e.g., Internet) networks?
- 77. In a multiple remote-site environment, are all sites maintained at the same security level?
- 78. Are the remote access physical topology and network maps documented, verified, and kept up-to-date?

Education/Awareness/Enforcement

- 79. Are users aware of the signs of a virus or worm?
- 80. Are users familiar with the use of virus scanners?
- 81. Are users aware of the dangers of software engineering?
- 82. Are users aware of the remote access security policies?
- 83. Do remote access users and their managers receive security training prior to using remote access?
- 84. Do remote access users and their managers receive annual security training?

Modem Access

- 85. Is there a single point of entry into the network (e.g., modem pool or terminal server)?
- 86. Are all modem phone numbers unlisted?
- 87. Is dial-out allowed at the corporate site?telework va

88. Does IP connectivity exist on individual corporate site systems?

89. Is auto-answer on dial-in access allowed at remote sites?

Copyright © 1999 American Health Information Management Association. All rights reserved.