ComplianceShield

Simplify and Streamline
Cyber Security Compliance

SAMPLE REMOTE WORKING SECURITY POLICY

Sample Information Security Template from Information Shield

This **Sample Security Policy Template** from Information Shield contains the essential controls for a remote working ("mobile working") information security policy.

It is offered as a benefit to eRiskHub® members and can be used to develop a policy for a single organization. The Template is one of over 40 offered as part of the ComplianceShield Security Subscription.

Streamline Cyber Security with ComplianceShield

ComplianceShield enables any business to quickly **define, deliver and demonstrate** a robust information security program that addresses essential regulatory and compliance requirements. With a simple user interface and expert information security guidance, ComplianceShield ™ integrates all of the essential security management functions into a single, integrated system that is easy to manage and deploy. ComplianceShield replaces months of manual effort using spreadsheets and expensive consultants with a simple software solution.

InformationShield

Information Shield
sales@informationshield.com
P: 888-641-0500
www.informationshield.com

Information Security Policies

Remote Working Security Policy

Policy #	CPL-XX	Effective Date	MM/DD/YYYY	Email	policy@companyx.com
Version	1.0	Contact	Policy Author	Phone	888.641.0500

Table of Contents

Customization Notes:

Organizations can customize this Security Policy Template based on their own business needs and risks. To customize: (1) replace the name “Company X” throughout the document with your organization’s official name, (2) remove the Information Shield logo with your own logo, and (3) replace the names, roles and dates in the policy header, Approval and Revision History.

PURPOSE

This policy defines the requirements for secure access to Company X information, networks and computing resources by authorized remote workers. This arrangement is also known as “teleworking” or “remote working”.

SCOPE

This policy applies to all Company X employees and Third-Party contractors with remote access to information systems and networks.

(Note: Organizations can change the scope of any policy to limit it to specific user groups, organizational units or even information systems. This policy applies to all personnel by default.)

POLICY

Required Approval

(This section addresses the need for remote working to be approved by management. The organization must be aware of which accounts are available for remote access.)

Remote Working Privileges – All employees working at home or at alternative sites must be specifically granted this privilege by the employee's manager or a member of the Information Technology Department.

Remote Working Agreement – All Company X employees who are approved to work from remote locations must first sign an agreement to abide by all Company X remote worker policies, procedures and standards. The agreement should be reviewed and signed annually.

(Note: ComplianceShield enables organizations automate the policy distribution and acknowledgement process via a secure web portal)

Compliance Requirements

(This section addresses the need for remote workers to adopt the same controls for policy compliance and intellectual property rights at remote locations.)

Software License Restrictions – Remote workers must follow software licensing restrictions and agreements on all software used to process Company X information at alternative work sites.

Remote Working Information Security Policies – Remote workers must follow Company X information security policies at remote work sites, including the Acceptable Use of Assets Policy.

Information Systems Security

(This section addresses the requirements to maintain secure configurations on all remote access equipment. Ideally, all personal systems with remote access to should be configured with at least anti-malware and personal firewalls. More advanced software is available to combat threats such as phishing and data leakage.)

Approved Remote Worker Equipment – Employees working on Company X business at alternative work sites must use Company X-provided computer and network equipment unless other devices have been approved by the Information Security Department.

Personally-Owned Information systems – Remote workers must not use their own mobile computing devices, computers, computer peripherals, or computer software for Company X teleworking business without prior authorization from their supervisor.

Malware Protection Software – All systems that access Company X networks remotely must have an anti-malware (anti-virus) package approved by the Information Security Department continually running.

Advanced Endpoint Protection – All systems that access Company X networks remotely must have an endpoint protection software package installed that protects the system from advances threats.

Setting Date and Time – Remote workers must diligently keep their remote computers' internal clocks synchronized to the actual date and time.

Remote Access Control

(Remote access must be carefully controlled and only through approved channels. Separate policies govern the establishment and configuration of remote access systems.)

Access Control System – Remote workers must not use a remote computer for Company X business activities unless this same computer runs an access control system approved by the Information Security Department.

Remote Access to Networks – All remote access to Company X networks must be made through approved Remote Access points that are controlled by the Information Technology Department.

Session Logout – After a remote worker has completed a remote session with Company X computers, the worker must log off and then disconnect, rather than simply disconnecting. Workers using remote communications facilities must wait until they receive a confirmation of their log off command from the remotely connected Company X machine before they leave the computer they are using.

Screen Positioning – The display screens for all systems used to handle Company X sensitive information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.

Sharing Access and Systems Prohibited – Remote workers must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or parameters with anyone without prior approval from the Information Security Department. This means that a remote computer used for Company X business must be used exclusively by the telecommuter. Family members, friends, and others must not be permitted to use this machine.

Alternative Work Sites

(Just like in traditional work environments, physical access to systems must be protected as much as possible. Physical protection includes both physical access and protection from environmental threats such as water damage.)

Alternative Work-Site Requirements – Before a remote working (telecommuting) arrangement can begin, the worker's supervisor or manager must be satisfied that an alternative work-site is appropriate for the Company X work performed by the involved worker.

Separate Room or Workspace – Whenever possible, remote working must be done in a separate room or workspace that can be locked or secured from the rest of the house or co-working space.

Inspections of Remote Working Environments – Company X maintains the right to conduct inspections of teleworker offices with one or more days advance notice.

Remote Working Environmental Controls – Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Lockable, Burglar-Resistant Furniture – All workers who must keep sensitive Company X information and mobile devices at their homes to perform their work, must receive from Company X—or otherwise provide—approved lockable cabinets or desks for the proper storage of this information.

Data Protection

(One of the great risks of mobile devices is accidental loss or theft. All sensitive data on remote systems should be encrypted either at the data or system level.)

Encryption and Boot Protection – All computers used for remote working (including portables, laptops, notebooks, and other transportable computers) which contain sensitive (Confidential or Secret) Company X information must consistently employ both hard disk encryption for all data files and boot protection through a password. These two essential controls must be provided through software or hardware systems approved by the Information Security Department [a link to list of approved information security products can be inserted here].

Backup and Media Storage

(Organizations should consider backup of data on remote systems if the data is not store on the network. This section should be modified based on the specific business situation.)

Backup Procedures – Remote workers are responsible for ensuring that their remote systems are backed up on a periodic basis, either automatically through the network or remotely with USB drives or similar equipment. If network backup is not available or feasible, Company X will provide telecommuters with local backup equipment.

Backup Media Storage – If backups are made locally, telecommuting workers must store copies of these same backups at a secure location away from the remote working site at least every two weeks. If these backups contain sensitive information, the backups must be encrypted using software approved by the Information Security Department [a link to list of approved information security products can be inserted here].

Sensitive Media Marking and Storage – When sensitive information is written external storage media (external drives, CD-RW, USB drive, etc.), the media must be externally marked with the highest relevant sensitivity classification. Unless encrypted, when not in use, this media must be stored in heavy locked furniture. Smart cards and tamper-resistant security modules are an exception to this rule.

Remote System Management

(The secure configuration of remote systems must be maintained. This section restricts users from making changes unless they are need and approved.)

Changes to Configurations and Software – On Company X-supplied computer hardware, workers must not change the operating system configuration or install new software. If such changes are required, they must be performed by Help Desk personnel with remote system maintenance software.

Changes to Hardware – Remote working computer equipment supplied by Company X must not be altered or added to in any way without prior knowledge and authorization from the Help Desk.

Information Disposal

(Information disposal is a key concern at remote locations. This applied both at a home workspace and also remote environments such as hotels or co-working spaces.)

Company X Property at Alternative Work Sites – The security of Company X property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable and prudent precautions must be taken to protect Company X hardware, software, and information from theft, damage, and misuse.

Provision of Secure Containers – Workers who must keep Secret or Confidential Company X information at their homes in order to do their work must have safes or lockable heavy furniture for the proper storage of this information. If these workers do not have such furniture or safes, Company X will loan these items to the telecommuting workers.

Shredders – Remote workers must have or be provided with a shredder to appropriately dispose of printed versions of sensitive information. Shredders that make strips of paper are not acceptable for the disposal of Company X sensitive material. Acceptable shredders make confetti or other small particles.

Paper Records Disposal – All printed copies of sensitive Company X information must be shredded for disposal. Telecommuting workers on the road must not throw away Company X sensitive information in hotel wastebaskets or other publicly-accessible trash containers. Sensitive information must be retained until it can be shredded, or destroyed with other approved methods.

System Ownership and Return

(This section applies to more long-term arrangements, where individuals may have systems or equipment that are issued by the organization. These controls can also be part of the Employment Termination Procedure.)

Return of Property – If Company X supplied a telecommuter with software, hardware, furniture, information or other materials to perform Company X business remotely, all such items must be promptly returned to Company X when a telecommuter separates from Company X, or when so requested by the telecommuter's manager.

Liability for Company X Property – If Company X supplied a telecommuter with software, hardware, furniture, information or other materials to perform Company X business remotely, Company X assumes all risks of loss or damage to these items unless such loss or damage occurs due to the telecommuter's negligence. Company X expressly disclaims any responsibility for loss or damage to persons or property caused by, or arising out of the usage of such items.

VIOLATIONS

(All published information security policies should address violations and non-compliance. This section should be reviewed by the Legal Department and approved by management.)

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does

not consider conduct in violation of this policy to be within an employee's or Third-Party's course and scope of employment, or the direct consequence of the discharge of the employee's or Third-Party's duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

DEFINITIONS

(Key definitions of terms used in the policy. These can be put in each policy or included in a global dictionary.)

Confidential Information (Sensitive Information) – Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a Third-Party under a non-disclosure agreement.

Information Asset – Any Company X data in any form that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and Third-Party data.

Information System – Any Company X equipment, applications or systems used to manage, process, or store Company X data. This includes, but is not limited to, information systems managed by third-parties.

Mobile Computing Devices – Mobile computing assets include, but are not limited to: laptops, notebooks, tablets, cell phones, and remote desktop computers. It also includes all portable storage media, including flash drives, smart cards, tokens, etc.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

Third-Party – Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

User – Any Company X employee or Third-Party who has been authorized to access any Company X electronic information resource.

REGULATORY REFERENCES

(This policy addresses requirements of the following information security frameworks and regulatory requirements. All Information Shield policy templates are mapped to multiple frameworks.)

CPL: 4.05.08 Teleworking
ISO/IEC 27002: 6.2.2 Teleworking
HIPAA: Device and Media - Accountability (A)
NIST: AC-17 Remote Access

PCI-DSS: 9.5 Physically Secure Media, 12.3 Acceptable Usage
US-CSFV: PR.AC-3: Remote access is managed

Related Documents

(This section references other policy documents that may be related to this document.)

Mobile Computing Security Policy
Remote Access Security Policy
Acceptable Use of Assets Policy

Approval and Ownership

Owner	Title	Date	Signature
Policy Author	Title	MM/DD/YYYY	
Approved By	**Title**	**Date**	**Signature**
Executive Sponsor	Title	MM/DD/YYYY	

Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	MM/DD/YYYY	MM/DD/YYYY	