Remote Work Policy Brought to You by Shred-it®

*(These Are Templates Only And Should Be Customized According To Your Organization's Information Security Requirements.)*

*(Insert your company logo in the blue box provided on the right by clicking the picture icon.)*

**STATEMENT OF POLICY:**



**Remote Work Policy**

**[Enter Your Company Name Here]**

**Workplace Policy#:** Enter Policy Number Here

**Effective Date:** Enter Date Here

**Issued by:** Enter Name Here

**Approved by:** Enter Name Here

1. **PURPOSE**

The purpose of this remote work policy is to assist [Enter Your Company Name Here] in managing confidential information when employees work remotely. This organization-wide policy will provide a clear and comprehensive outline   
of information security practices, remote working requirements, and tips on   
how to remain productive while working remotely.

This policy will help ensure that [Enter Your Company Name Here] employees:

* Know how to reduce the threat of a security breach
* Protect the confidential information of our customers, our company, and each other
* Remain productive while working away from the office

Implementation of and compliance with this policy is essential to its effectiveness. Incomplete or selective implementation may expose [Enter Your Company Name Here] to legal and security risks. Therefore, each employee must understand and cooperate in the implementation and enforcement of the policy.

**Policy Administration**: Should any questions, comments, or suggestion arise regarding this policy, please contact [Insert Team And Contact Information Here].

1. **SCOPE**

This policy will apply to paper and digital documents, confidential information, general business information (as defined in Section 4 below), and the data of all employees employed at [Enter Your Company Name Here] or to which [Enter Your Company Name Here] is a party or signatory.

1. **RESPONSIBILITIES**

**Senior management** is responsible for ensuring that this policy is adhered to by their respective departments. One member of senior management is to be appointed as the Document Control Administrator (DCA) with the responsibilities outlined below. Other members of senior management are responsible for applying this policy within their areas of responsibility.

The role of **DCA** currently assigned to [Enter The Name Of The Position Responsible] should advise and direct the implementation of this policy, including ensuring all employees are aware of it and have been trained on how to comply with it. It is also his/her responsibility to ensure that they work with IT to provide employees with access to the appropriate infrastructure (e.g., secure VPN, communication methods, and remote access tools) that they will require to work remotely.

**Employees**: All [Enter Your Company Name Here] employees are responsible   
for complying with this policy.

1. **DEFINITIONS**
   1. **Documents**: These refer to all business documents of [Enter Your Company Name Here], including written, printed, and digital. Documents include, but are not limited to, papers, photocopies, drafts, bound records, drawings, maps, photographs, electronic communications, and any other physical devices containing information, including electronic storage devices. The term includes any and all copies or originals taken, moved, or sent off any [Enter Your Company Name Here] site and are within [Enter Your Company Name Here] control.
   2. **Public Information:** Refers to any and all electronic storage devices that were provided by or contain information that is the property of [Enter Your Company Name Here], are under [Enter Your Company Name Here] control, and are used by any of its employees, contractors, officers, or directors. Electronic storage devices include personal computers, servers, laptops, and related storage devices such as hard drives, flash drives, and CDs.
   3. **Electronic Storage Device**: This refers to any and all electronic storage devices that were provided by or contain information that is the property of [Enter Your Company Name Here] , are under [Enter Your Company Name Here] control and are used by any of its employees, contractors, officers, or directors. Electronic storage devices include personal computers, servers, laptops, and related storage devices such as hard drives, flash drives, and CDs.
   4. **Remote Work:**This is defined as any time an employee of [Enter Your Company Name Here] works away from the office. This can involve working from home or anywhere where they may not receive the same security or access that they would at work.
2. **Remote Work Guidelines**

It is every employee of this company’s responsibility, in accordance with privacy protection legislation, to protect the confidential information of our business, its employees, partners, and clients. Confidential information should only be taken home if absolutely necessary.

1. **Storage and Usage of Tangible Documents with Confidential Information**All documents whether on-site or off-site should be stored in locked cabinets. All confidential information must be kept out of view from unauthorized personnel and locked up when not in use. Any paper produced at home, that is not in immediate use, should be destroyed at the workplace or in a secure recycling console.
2. **Storage and Usage of Digital Documents with Confidential Information**If an employee is accessing and printing company files on a home computer,   
   all computer security software must be up to date. Additionally, all employees   
   must be trained on appropriate storage methods and password protection   
   techniques to help ensure their documents remain secure. If any digital devices,   
   such as phones or USB drives, are used for storage or access, they must be encrypted to allow for maximum security.
3. **Remote Access for Employees**Since employees will be working away from the office, they must have the same access that they have when they are in the workplace. The DCA must work with the IT department to help ensure that appropriate and secure remote access methods are available when employees are working off-site. All employees must use only approved methods to connect to the network. In addition, managers in each department must emphasize the importance of leaving all communication channels (e.g., instant messenger, cell phone, email) open so that they can be reached when needed.
4. **Breach Notification Process**  
   If a breach does occur when employees work remotely, the incident will need to be investigated by the proper teams to determine if a breach did indeed occur and to remediate any issues identified. Employees should contact their manager and the Service Desk or Help Desk. This way, an audit can be completed to assess the damage and identify additional areas of risk and corrective action can be taken as necessary to protect the data from being compromised further.