A close up of a logo

Description automatically generated



**Remote Working Policy Template**

Ensure Employees Follow Proper Security Protocol While Working from Home

Table of Contents

[Purpose of This Document 3](#_Toc37056966)

[Remote Working Policy 3](#_Toc37056967)

[Scope 3](#_Toc37056968)

[Responsibilities 3](#_Toc37056969)

[Remote Secure Area Risk Assessment 3](#_Toc37056970)

[Remote Working Procedures 4](#_Toc37056971)

[Passwords 4](#_Toc37056972)

[Clear desk policy, screen savers and information reproduction 5](#_Toc37056973)

[Software 5](#_Toc37056974)

[Data control and legislation 5](#_Toc37056975)

[Backup and information classification 5](#_Toc37056976)

[Maintenance, insurance and return of equipment 6](#_Toc37056977)

[Acceptable Use 6](#_Toc37056978)

[Introduction 6](#_Toc37056979)

[Equipment Acceptable Use 6](#_Toc37056980)

[Internet Acceptable Use 7](#_Toc37056981)

[Email Acceptable Use 7](#_Toc37056982)

[Document Owner and Approval 7](#_Toc37056983)

[Change History Record 7](#_Toc37056984)

[About Prevalent 8](#_Toc37056985)

# Purpose of This Document

This document was prepared to provide Prevalent customers and the broader risk management community with a free example of a remote working policy to address best practices for security. We hope this resource helps to formalize security policies for newly remote working employees as a result of the current pandemic.

# Remote Working Policy

## Scope

All remote workers who use organizational assets to connect to organizational facilities or networks are subject to the requirements of this policy.

## Responsibilities

Once all the prerequisites for setting up a remote working site have been completed, authorization of remote worker access follows the same procedure as established for office-based users.

* The [Person Responsible] is responsible for the configuration of required computing equipment.
* The [Person Responsible] is responsible for network configuration and for providing remote network connectivity and user support.
* The [Person Responsible] is responsible for the site survey and implementation of necessary physical improvements and controls.
* The [Person Responsible] is responsible for any new equipment purchased.
* The [Person Responsible] is responsible for the risk assessment.
* The [Person Responsible] is responsible for ensuring that insurance requirements are met.
* Remote workers have specific responsibilities, as set out in their User Agreements.

## Remote Secure Area Risk Assessment

The proposed site must be surveyed, and the risks assessed before a decision can be made as to whether or not to authorize creation of a remote worker facility; and if it is to be authorized, to decide what controls will be necessary.

The findings of the site survey and the details of the requirements should be gathered and used as inputs to a risk assessment. The risk assessment determines the controls that are necessary for each teleworking location. The [Person Responsible] documents the required controls in the output from the risk assessment.

The remote working site is brought into conformity with the required specification, in terms of any necessary physical security improvements, and the provision of home network and connectivity infrastructure.

Any necessary changes to the network are made to ensure that [Organizations name] access control policy is not breached by the remote worker. Once these steps have all been accomplished, the remote worker facility can be authorized.

The remote worker undergoes necessary training and then signs a remote worker User Agreement which sets out all the obligations and requirements in respect of the teleworking facility.

## Remote Working Procedures

The [Organizations name] requires:

* All laptops to have firewalls enabled, anti-malware software installed, and automatic updating facilities to be up to date and that they meet the corporate minimum standards.
* All users should follow corporate policy on usernames and passwords, to ensure a password protected screensaver is in place, all folders containing confidential corporate information are encrypted, and folder and printer sharing has been disabled.
* All users’ laptops should be physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft, the specified corporate policy for dealing with such incidents is followed.
* All users must ensure that the most recent operating system and application security-related patches, fixes and updates have been installed.
* All laptops should be backed up in line with corporate policy.

Users must comply with the corporate requirements [detail where this can be found] on the means of connecting to public access points and accessing corporate systems.

## Passwords

Usernames and passwords will be issued in line with [Organizations name]’s procedure for authorizing and issuing them.

* Initial temporary passwords must be changed at first logon.
* Use passwords that are at least 8 characters in length, are alpha-numeric, are not based on any easily guessable or memorable data such as names, dates of birth, telephone numbers etc., are not dictionary words and are free of consecutive identical all-numeric or all-alphabetic characters.
* Users will keep passwords secret and will not under any conditions divulge them to or share them with anyone, nor write them down or leave them anywhere where they can easily be found by someone else and recorded.
* Passwords must not be stored in any automated logon process.
* Password must be changed at intervals as required by [Organizations name] and users must not attempt to re-use passwords or use new passwords that are in a sequence and must change passwords more frequently if there is evidence of possible system or password compromise.
* Users must not use the same password for organizational and personal use.
* Replacement passwords are administered by [Person Responsible]; users must obtain the written permission of their [Person Responsible] before a replacement password can be issued.
* Connectivity for remote access will be [explain the connectivity provided for remote access i.e. VPN, 2-factor authentication etc.].

## Clear desk policy, screen savers and information reproduction

* Users should ensure that no confidential or restricted information (in paper or removable storage media format) is left on desks, or left in or near reproduction equipment (photocopiers, fax machines, scanners, etc.).
* Users should ensure that a password protected screensaver is in place that operates within [state frequency] minutes of no activity or manually activated when the workstation is left unattended.
* Active computer sessions should be deactivated when finished and logged off (i.e. not simply turn off the computer screen) when work is completed.
* Personal storage media, MP3 players, digital cameras and mobile phones with photographic capability should not be used.
* Use of the Organizations reproductive equipment (photocopiers, fax machines, scanners) should be used, appropriate to the classification level of any information being reproduced.

## Software

* Users must not disable or over-ride any of [Organizations name]’s installed software, including anti-malware software, firewalls and automatic updating services.
* Users may not download from the Internet or install on any organizational computer or other device any software of any sort for which [Organizations name] does not have a valid license and that has not had the prior authorization of the [Person Responsible]. This prohibition includes freeware, shareware, screensavers, toolbars and/or any other programs that might be available.
* The use of Instant Messenger facilities is[Describe the process]and users will abide by it.

## Data control and legislation

* Users must obtain the written authorization of the [data protection officer or person responsible] for the storage of any personal information on [Organizations name]‘s computer systems.
* Users must abide by any legal requirements with respect to computer use, including privacy and data protection regulations.

## Backup and information classification

Users are responsible for ensuring that all information on laptops is correctly classified and labeled in line with the requirements of the Classification Policy.

[Detail encryption requirements]

Users are responsible for backing up information on laptops in line with organizational requirements [detail the requirements for backup].

## Maintenance, insurance and return of equipment

[Detail any maintenance/Insurance and return of equipment (starters/leavers process)].

# Acceptable Use

## Introduction

The Internet is an unregulated environment. [Organizations name] will not be liable for any material viewed or downloaded. Use of the Internet must be consistent with [Organizations name] standards of business conduct and must occur as part of the normal execution of the employee’s job responsibilities. Any breach may lead to disciplinary action and possibly termination of employment. Illegal activities may also be reported to the appropriate authorities.

As per this policy, “users” include all staffof [Organizations name] as well as contractors, temporary staff and third parties that are granted access to organizational information assets.

## Equipment Acceptable Use

* Organizational user IDs, websites and e-mail accounts may only be used for organizationally sanctioned communications.
* Use of Internet/intranet/e-mail/instant messaging [may/will] be subject to monitoring for reasons of security and/or network management and users may have their usage of these resources subjected to limitations by the [Organization’s name].
* The distribution of any information through the Internet (including by e-mail, instant messaging systems and any other computer-based systems) may be scrutinized by [Organization’s name] and [Organization’s name] reserves the right to determine the suitability of the information.
* The use of organizational computer resources is subject to GDPR law and any abuse will be dealt with appropriately.
* Users will not seek to avoid and will uphold [Organizations name]’s anti-malware policy and procedure, will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and will not examine, change or use another person’s files or any other information asset for which they don’t have the [owner]’s explicit permission.
* Users will not carry out any other inappropriate activity as identified from time to time by [Organizations name] and will not waste time or resources on non-organization business. This includes downloading bandwidth intensive content such as streaming video and MP3 music files, sharing digital photographs, etc.

## Internet Acceptable Use

* Users may not visit Internet sites that contain obscene, hateful or other objectionable material, shall not attempt to bypass organizational surf control technology and shall not make or post indecent remarks, proposals or materials on the Internet.
* Users may not download software from the Internet or execute or accept any software programs or other code on the Internet unless it is in accordance with [Organizations name]’s policies and procedures.

## Email Acceptable Use

* Users shall not solicit e-mails that are unrelated to business activity or which are for personal gain, shall not send or receive any material which is obscene or defamatory or which is intended to annoy, harass, or intimidate another person, and shall not present personal opinions as those of the company.
* Users may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties, may not reveal or publicize confidential information, and will not send confidential e-mails without the level of protection detailed in the Classification Policy.

## Document Owner and Approval

The [Person Responsible] is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the information security policy.

This procedure was approved by the [Person Responsible] and is issued on a version-controlled basis under his/her signature.

Signature: Date:

# Change History Record

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue |  |  |
|  |  |  |  |
|  |  |  |  |

# About Prevalent

Prevalent helps enterprises manage risk in third-party business relationships. It offers the industry’s only purpose-built, unified platform that integrates a powerful combination of automated assessments, continuous monitoring, and evidence sharing for collaboration between enterprises and vendors. No other product on the market combines all three components, providing the best solution for a highly functioning, effective third-party risk program.

To learn more, please visit [www.prevalent.net](http://www.prevalent.net).

© Prevalent, Inc. All rights reserved. The Prevalent name and logo are trademarks or registered trademarks of Prevalent, Inc. All other trademarks are the property of their respective owners. 04/20