These sample documents are not intended to be adopted in their current form by any company. Codestar, Inc does not warranty the appropriateness of these sample policies for any use.

The sample documents are based on a fictitious company that needs to comply with state data breach and privacy laws, but does not need to comply with an industry standard such as HIPAA, FERPA, PCIDSS, etc.

You will notice that this policy prohibits many uses of wireless devices (in sections IV and V), which reduces the risk and also allows for a simpler policy and training. A company that permits its personnel to use their own devices will need a policy that includes additional topics and rules.

Sample
Acceptable Use Policy for Portable Wireless Devices

Introduction
This policy outlines the standards for use of portable wireless devices, which Sample Org, Inc. requires all personnel to follow.

What is covered by the Policy?
The use of portable wireless devices, including laptops, tablet computers, and smartphones.

Who is covered by the policy?
All employees, volunteers, and contracted onsite workers are covered by this policy. (Contractors who do occasional or offsite work for Sample Org should refer to their contract terms for guidance specific to their roles.)

I. **Purpose**
It is the policy of Sample Org, Inc. to maintain effective IT security in order to protect the privacy of its data and thereby of its staff, volunteers, clients, and other stakeholders. To this end, we provide the following policy and rules which govern the use of portable wireless devices by all personnel.

II. **Rights and Responsibilities of Sample Org**
Sample Org retains the following rights and recognizes the following obligations:
   A. To log network use and online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
   B. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to restrict online destinations through software or other means.
   C. To provide guidelines and make reasonable efforts to train personnel in acceptable use and policies governing wireless device use.
   D. To appoint a staff person as the contact for issues and questions related to this policy.

E. To keep this policy and associate rules updated and relevant to current technology and business activities.

III. **Rights and Responsibilities of Personnel**

Personnel who sign off on this policy are affirming their following rights and obligations:

A. To understand and adhere to this policy and its rules.
B. To request and receive training, review, or clarification on these policies as needed.
C. To use portable wireless devices only in ways that comply with this policy and its rules.

IV. **Portable wireless devices owned by the individual**

A. Personnel who own a portable device may use it to access their company email account via the webmail app.
B. No other company business may be carried out on a device owned by the user.
C. When accessing the webmail application at our facility, users may connect to the passworded guest wifi.
D. When using webmail off company grounds, the user must connect via their mobile data plan, NOT via a wifi hot spot.
E. Users shall not download attached files to their personal device.
F. Webmail login password shall not be saved on the device; it must be entered each time.

V. **Portable wireless devices owned by Sample Org, Inc.**

A. Personnel whose job requires use of a portable wireless device will be provided with an encrypted company-owned device.
B. Users shall not modify the security settings of company-owned devices.
C. Company-owned devices may be used to connect to the internal wifi network.
D. Such devices shall not be used to connect to any public wifi hotspot that is not password-protected.
E. Employees may check a personal email account using the company-owned device, but may not open any links or attachments from their personal email on this device.
F. Such devices shall not be used for any activity that is not related to the business of Sample Org, Inc. Specifically excluded are:
    1. Downloading games, movies, or other non-business-related software.
    2. Carrying out any commercial or political activity that is not Sample Org business
    3. Carrying out any activity which is illegal or which infringes third party rights or is otherwise harmful.
    4. Accessing sites which are for gambling, pornography, illegal filesharing, or games unrelated to their work.
G. Devices may be inspected for compliance periodically.

VI. **Passwords**

Poor password management could compromise Sample Org's entire network. All personnel are responsible for taking the appropriate steps to select and secure their passwords for devices and applications.

A. Each user must be provided with their own unique login account to all devices, software programs, and web applications.

A. Users shall not share their password with anyone else, or ask other personnel for passwords.
B. Users shall not use the same password for multiple applications
C. Users shall not store passwords on any computer in an unencrypted file.
D. Passwords should:
    1. Be at least 8 characters
    2. Include letters and numbers or symbols

3. Include uppercase and lowercase letters

B. Passwords should not:

1. Be a pattern (qwertyui, a1a1a1a1a1a1, or t00t00t00)
2. Be a single word
3. Be a date, address, phone number, name, or other fact that is associated with the company or the individual.
4. Be a word spelled backwards

VII. **Reporting**

The IT Director is our designated point person for reporting security and data breach issues. The manager of the IT Director is a backup contact if needed.

A. Users shall *immediately* report a theft of any company device that stores data. Do not wait until regular business hours to report this.
B. Report questionable email attachments and links and get advice before opening them.

VIII. **Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action.

User Agreement (to be signed by all personnel)

I have read, understand, and will abide by the above Acceptable Use Policy and its rules. I have had an opportunity to ask questions about any policy items I did not understand. I further understand that any violation may result in revocation of access privileges, disciplinary action, and/or appropriate legal action.

User Name (please print):

User Signature: Date:

A WiFi Acceptable Use Policy is generally shown in the Internet browser window when a user attempts to connect. Usually there is an "Accept" button which must be clicked before the connection proceeds.

Sample
Acceptable Use Policy for Guest WiFI Access

Sample Org, Inc. provides you access to its WiFi network providing you agree to abide by this policy.

Introduction

This policy outlines the standards which Sample Org requires all users of its Guest Wifi network to follow.

What is covered by the Policy?
The use of the Guest WiFi network supplied by Sample Org.

Who is covered by the policy?
This policy covers all individuals who wish to use the WiFi network supplied by Sample Org.

Internet Use
While using our network you agree not to visit sites that are, or transmit information that is:
– Illegal under current law
– Defamatory, threatening or intimidating, or which could be classed as harassment
– Pornographic, whether writing, pictures, films or video clips
– Infringement on third party rights, such as copyright and digital rights

Internet Content
Sample Org reserves the right to block access to any site.

Systems and Data Security
Sample Org will provide Internet access via the wireless network and will take reasonable steps to ensure it is secure from unauthorized users. However, no guarantee can be made to this effect. You are responsible for your own anti-virus and anti-malware precautions. Sample Org will not be held responsible for any damage to your equipment while connected to its network.

You should not attempt to gain access to restricted areas of the network or to any password protected information without being authorized to do so.

Monitoring and Compliance
Sample Org reserves the right to protect its network and systems by logging the sites accessed by users. However, we will not record the content of your activity.

We do this to:
- ensure the use of the system is legitimate and in compliance with this policy
- to comply with our legal obligations and policies

If your use of the network is in violation of our policy, we reserve the right to terminate your access.
If your use of our network appears to involve a criminal offense, we will notify the police.

Specific Permissions to you
Wireless access to the Internet in accordance with this policy.

Use of the WiFi network provided by Sample Org infers your acceptance of this policy.