# PDA Usage Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to define standards, procedures, and restrictions for connecting to [Company Name’s] internal network(s) or related technology resources via any means involving mobile devices that are categorized as Personal Digital Assistants (PDAs).

The overriding goal of this policy is to protect [Company Name’s] technology-based resources (such as corporate data, computer systems, networks, databases) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing PDA-based technology to access corporate technology resources must adhere to company-defined processes for doing so.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions i.e. those people, elements or situations that are not covered by this policy or where special consideration may be made.

* This policy applies to, but is not limited to, all devices that fit the following device classifications:
* Handhelds running the [PalmOS, Microsoft Windows CE, PocketPC or Windows Mobile, Symbian, or Mobile Linux] operating systems.
* Mobile devices that are standalone (i.e. connectible using wired sync cables and/or cradles.)
* Devices that have integrated wireless capability. This capability may include, but is not limited to, [Wi-Fi, Bluetooth, and IR.]
* Smartphones that include PDA functionality.
* Any related components of [Company Name’s] technology infrastructure used to provide connectivity to the above.
* Any third-party hardware, software, processes, or services used to provide connectivity to the above.
* The policy applies to any PDA hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.
* This policy applies to all [Company Name] employees, including full- and part-time staff, contractors, freelancers, and other agents who utilize company-owned, personally owned, or publicly accessible PDA-based technology to access the organization’s data and networks via wired and wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at [Company Name] does not automatically guarantee the granting of these privileges.
* Addition of new hardware, software, and/or related components to provide additional PDA-related connectivity within corporate facilities will be managed at the sole discretion of IT. Non-sanctioned installations of PDA-related hardware, software, and/or related components, or use of same within the organizational campus, or to gain access to organizational computing resources, are strictly forbidden.
* This policy is complementary to any previously implemented policies dealing specifically with network access, wireless access, and remote access to the enterprise network.

# Definitions

Define any key terms, acronyms or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. **PDA (Personal Digital Assistant).** This is defined as a handheld computing device that contains telephone, internet, and networking features.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. All PDAs and related connectivity points within the corporate firewall will be centrally managed by [Company Name’s] IT department and will utilize encryption and strong authentication measures. Although IT is not able to manage the public network to which wireless-enabled PDA devices and smartphones initially connect, end users are expected to adhere to the same security protocols while using this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company’s infrastructure.
2. The following table outlines [Company Name’s] minimum system requirements for a computer, workstation, or related device to properly support and sustain PDA connectivity and functionality. Equipment that does not currently meet these minimum requirements will need to be upgraded before PDA implementation may be sanctioned by IT.

###### **Desktop/Laptop Minimums for PDA Installation**

**PalmOS:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | PC and PC-Compliant Computers | **Macintosh Computers** | **Other Client OS/Environment (As Applicable)** |
| Operating System |  |  |  |
| CPU |  |  |  |
| RAM |  |  |  |
| Disk Space |  |  |  |
| Email Client Version |  |  |  |

**Microsoft Windows CE, PocketPC, Windows Mobile:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | PC and PC-Compliant Computers | **Macintosh Computers** | **Other Client OS/Environment (As Applicable)** |
| Operating System |  |  |  |
| CPU |  |  |  |
| RAM |  |  |  |
| Disk Space |  |  |  |
| Email Client Version |  |  |  |

**Other Mobile OS (Please Specify):**

|  |  |  |  |
| --- | --- | --- | --- |
|  | PC and PC-Compliant Computers | **Macintosh Computers** | **Other Client OS/Environment (As Applicable)** |
| Operating System |  |  |  |
| CPU |  |  |  |
| RAM |  |  |  |
| Disk Space |  |  |  |
| Email Client Version |  |  |  |

###### **Approved PDA Devices**

|  |  |  |  |
| --- | --- | --- | --- |
|  | PC and PC-Compliant Computers | **Macintosh Computers** | **Other Client OS/Environment (As Applicable)** |
| [Handheld Manufacturer] |  |  |  |
| [Handheld Model Number] |  |  |  |
| [Additional Handheld Manufacturer – as applicable] |  |  |  |
| [Additional Handheld Model Number – as applicable] |  |  |  |

Note: Fill in device information in the left-hand column. Check off supported platforms in the boxes to the right.

1. All employees requiring the use of PDAs for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should their application be accepted. Application forms must be approved and signed by the employee’s unit manager, supervisor, or department head before submission to the IT department.
2. Employees may use privately owned PDAs (under “Supported Technology”) for business purposes. If this is the case, the IT department must approve the specific handheld and connection type as being secure and protected. However, the company’s IT department cannot and will not technically support third-party wireless hardware or software, or any other unapproved remote email connectivity solution.
3. All expense forms for reimbursement of cost (if any) incurred due to the need for PDA-based access for business purposes must be submitted to the appropriate unit or department head. Financial reimbursement for PDA devices and related equipment is not the responsibility of the IT department. If you foresee an upcoming need for PDA use in a business context, ask your leader to help you fill out a business case.
4. It is the responsibility of any employee of [Company Name] who is connecting to the organizational network via a PDA to ensure that all components of their connection remain as secure as their network access within the office. It is imperative that any wired (via sync cord, for example) or wireless connection, including, but not limited to PDA devices and service, used to conduct [Company Name] business be utilized appropriately, responsibly, and ethically.
5. Employees using PDAs and related software to connect to [Company Name’s] technology infrastructure will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with [Company Name’s] password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
6. All PDAs that are used for business interests, whether personal or company-owned, must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, power-on passwords. Any non-corporate computers used to synchronize with PDAs will have installed whatever antivirus software deemed necessary by [Company Name’s] IT department. Antivirus signature files must be updated in accordance with existing company policy.
7. Passwords and other confidential data as defined by [Company Name’s] IT department are not to be stored on PDAs or their associated storage devices.
8. Due to the potential for bandwidth conflicts within [Company Name], use of unsanctioned equipment operating within the [2.4 GHz] range is strictly forbidden. If you have a need to use such equipment – for example, a wireless PDA or smartphone – please consult IT before proceeding further.
9. Prior to initial use for connecting to the corporate network, all PDA-related hardware, software, and related services must be registered with IT. A list of approved devices, software, and related services is available for viewing at [web address]. If your preferred PDA solution does not appear on this list, contact the help desk at [email address] or [phone number] to have it registered and added to the list.
10. Remote users using non-corporate network infrastructure to gain access to corporate resources via their PDAs must employ for their devices and related infrastructure a company-approved personal firewall, VPN, and any other security measure deemed necessary by the IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with [Company Name’s] additional security measures. IT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.
* For wireless-enabled PDAs, users must deactivate their devices when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
* Users must apply new passwords every business/personal trip where company data is being used on, or synchronized to, a PDA.
1. Any PDA that is configured to access [Company Name] resources via wireless or wired connectivity must adhere to the authentication requirements of [Company Name’s] IT department. In addition, all hardware security configurations (personal or company-owned) must be approved by [Company Name’s] IT department.
2. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of [Company Name’s] IT department. This includes, but is not limited to, installation of PDA software on company-owned desktop or laptop computers, connection of sync cables and cradles to company-owned equipment, and use of company-owned wireless network bandwidth via these devices.
3. [Company Name] will maintain a list of approved PDA-specific software applications and utilities, and it will be stored [file location or URL].
4. Employees, contractors, and temporary staff with [Company Name]-sanctioned wireless-enabled PDAs must ensure that their computers and handheld devices are not connected to any other network while connected to [Company Name’s] network via remote access.
5. All connections that make use of wireless PDA access must include a “time-out” system. In accordance with [Company Name’s] security policies, sessions will time out after [xx] minutes of inactivity, and will terminate after [xx] hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks through a wireless PDA connection.
6. The PDA-based user agrees to immediately report to his/her manager and [Company Name’s] IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.
7. The PDA-based wireless access user also agrees to and accepts that his or her access and/or connection to [Company Name’s] networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
8. [Company Name] [will/will not] reimburse employees for business-related wireless PDA-based access connections made on a pre-approved privately owned internet service provider service. All submissions for reimbursement must be accompanied by sufficient and appropriate documentation (e.g. original service bill). Employees requesting reimbursement will also be asked to certify in writing prior to reimbursement that they did not use the connection in any way that violates company policy.
9. Any questions relating to this policy should be directed to [Name] in IT, at [phone number] or [email address].
10. IT reserves the right to turn off without notice any access port to the network that puts the company’s systems, data, users, and clients at risk.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.