# Plus91 IT Policies

Authors: Aditya Patkar, Ajay Mandera

Version No: 0.2

## CONFIDENTIAL

**This document is for Specifically Authorized Personnel Only. The information contained herein is the proprietary of Plus91 Technologies Pvt. Ltd. and any other use or disclosure of such information is prohibited. This report shall not be reproduced, copied or used in whole or in part without prior written approval of Plus91 Technologies Pvt. Ltd**

## Revision History

| Revision | Date | Reason for Change | Author |
|---|---|---|---|
| 0.1.0 | 20-08-2020 | Initial Draft | Ajay Mandera |
| 0.2.0 | 17-04-2021 | Addition of Laptop Policy | Ajay Mandera |

# Table of Contents

# Definitions and Abbreviations

| | |
|---|---|
| Server | A computer or device which provides services over a network and is configured to allow access by multiple users. |
| Development team | A team of software developers, who work on the application and do the coding. |
| Jump Server | Jump Server is an intermediary server, which will help to connect the application or database server where direct access of the servers is not allowed. |
| PHI | Protected health information |

# Laptop Policy

**Purpose**

The purpose of this policy is to protect laptops from being damaged and keep them (including the data inside) secure, ensuring that users are aware about laptop usage in Plus91.

This policy addresses the actions that must be taken by all Plus91 employees who have a company-issued laptop.

**Protection**

Laptops should not be used in environments that might increase the likelihood of damage.Laptops should be kept in a padded carrying case or sleeve during transportation.

The physical security of Company provided laptops is the employee's personal responsibility. He/she is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.

**Software Installations**

Do not download, install or use unauthorized softwares or unknown web applications. Any software that is required to be installed must be installed through the IT person. A list of approved software is maintained in Appendix A.

**Inappropriate materials**

Plus91 Technology will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites.

### Health and Safety aspects

Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Where possible, place the laptop on a conventional desk or table.

### Virus Protection

Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person. Avoid clicking unknown links received in the email.

Always virus-scan any files downloaded to your computer from any source (USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically if your virus definitions are up to date, but you can also initiate manual scans if you wish to be certain.

For the Ubuntu operating system, make sure running softwares are up to date, if not contact the IT team. Work on a trusted network, avoid running unknown and unnecessary services. Check service logs if found suspicious or contact the IT team.

Report any security incidents (such as virus infections) promptly to the IT Team in order to minimize the damage

Respond immediately to any virus warning message on your computer, or if you suspect a virus or suspicious file/activity, contact the IT team immediately.  Do not forward any files or upload data onto the network if you suspect your PC might be infected.

### Data Security

Employees are expected to ensure the security of the data within their laptops. In this regard you are to adhere to the following:

- You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret.  Never share it with anyone, not even members of your family, friends, or IT staff.
- Corporate laptops are provided for official use for authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.

- Avoid leaving your laptop unattended and logged-on.  Always shut down, log off or activate a password-protected screensaver before walking away from the machine.
- Employees must use an office laptop for office work.

**Damage and Loss**

In case of any failure, employees are required to report the same to the management.

In case of the loss of laptop- be it on, or off Company premises, due to negligence of the employee, Plus91 may recover the cost of the laptop from the employee. It is the Company's discretion to impose further penalties on account of loss of sensitive Company information.

If there is damage on account of the above the employee may be liable to pay the damages at cost to the Company/the same may be deducted from their monthly salary.

In case of leaving the employment or being terminated for any reason, the employee will hand over the asset to the IT Team in good condition, failing which the Plus91 is authorized to charge a penalty or take legal action against the employee.

# Server Policy

### Purpose

The purpose of this policy is to outline Plus91 for administering servers that will ensure an acceptable risk posture against real-world threats concerning usage and access of servers. The aim is to restrict the access control and usage of servers. All selective members of, IT Team and The Development Team of the project are participants of the policy.

### Server Access

- Development team will get limited access to the servers.
- The IT Team will provide Server credentials to the Senior developer in the project.
- It is the Senior developer's responsibility to make the access credentials confidential.
- If the Senior developer wishes to share the credentials with another team member, he/she must get permission from a Privacy officer or appropriate person.
- During the active session on servers, all executed commands will be logged.
- Access to servers must be made from the Plus91's network or from a secure network or from Jump servers.
- Server credentials sharing must be limited to the IT team and Development team, sharing with other team members including but not limited to Testing or support team is strictly prohibited.

### Server Usage

- Developers are not the only one using the server, keep the server clean. Do not create trash or temp files on the server.
- Developers are only allowed to use the application folders with non-sudo privileges.
- During the active session, if noticed unusual on the server including slowness or any suspicious activity, the incident must be reported to the IT team immediately.
- Server to Server, Data must be transferred via SFTP or HTTPS.
- While using Jump server for Live server access, no PHI data must be downloaded to Jump Server.

**Server Security**

- Server credentials must not be shared, written down on paper,stored within a file or database on a workstation or on a jump server and must be kept confidential.
- Do not use any unauthorized or unapproved third party softwares for making connections to servers.
- If working on the Jump server, do not keep SSH/MySQL/Web sessions open to the live server. If anyone is found doing so, strict action will be taken.

**Server Abuse**

- Any attempt to undermine or cause harm to a server, or PHI Data is strictly prohibited. It will be considered as a serious violation of server policy and strict action will be taken.
- Unauthorized use of other accounts or file systems on the server is strictly prohibited.
- Malicious activities including but not limited to running malicious scripts/code, password robbery, security hole scanning or doing damage on server intentionally are seen as a serious violation of server policy and strict action will be taken.

# Data Policy

Plus91 shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been accessed, altered or destroyed in an unauthorized manner.

**Purpose:**

The purpose of this policy is to protect Plus91's ePHI from improper access, alteration or destruction. This policy applies to all data including but not limited to patient information, IT Systems information, financial information or human resource data.

The Plus91 must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting the clients, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

**Access Control Authorization**

- Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the IT department.
- Passwords are managed by the IT Service Desk. Requirements for password length, complexity and expiration are stated in the company password policy.
- Each team will have the unique user and password to access the project on Live server. These credentials should not be shared with unauthorized people in Plus91 or outside.
- Accessing the unauthorized data on the server or any other storage devices of Plus91 is strictly prohibited, if found doing so an action will be taken.

## User Responsibilities

- All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
- All users must keep their workplace clear of any sensitive or confidential information when they leave.
- All users must keep their Pc’s passwords confidential and not share with anyone.
- Please keep a clean desk. To maintain information security, you need to ensure that all printed data is not left unattended at your workstation/Desk.
- You must inform the IT team in the event of but not limited to any data loss or damage to the device/workstation of the Plus91.
- If you find a system or process which you suspect is not compliant with this policy or the objective of information security, it is your duty to inform the IT Team or your manager.
- Do not click on suspicious links or open attachments that can lead to malware attacks.

## Application and Information Access

- All Plus91 users shall be granted access to the data and applications according to their job roles, manipulation of access privileges is considered as violation of the policy.
- Users shall access sensitive data and systems only if there is a business need to do so and have approval from their project manager.
- Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.
- Users must drop an email to the IT team with your manager’s consent for remote access to the workstation in the office. Accessing your workstation from home without approval is not allowed.

## Access to Confidential, Restricted information

- Access to data classified as ‘Confidential’ or ‘Restricted’ shall be limited to authorized persons whose job responsibilities require it, as determined by the privacy officer or higher management.
- The responsibility to implement access restrictions lies with the IT Security department and higher management.

- Intentionally sharing data including but not limited to PHI, business and other private information of Plus91 to unauthorised users in Plus91 or outside people is a punishable offence and appropriate action will be taken.
- Tablet and smartphones - No PHI or confidential information should be stored on smart devices. Plus91 shall also employ remote wipe technology to remotely disable and delete any data stored on a tablet or smartphone which is reported lost or stolen.

**PHI Data management**

Access:

- Users can not download or access patient data on personal or office workstations.
- IT team will provide a cloud workstation for each team to access PHI data.
- The project manager will have full access to this cloud workstation.
- It is the project manager's responsibility to make the access credentials confidential, if the credentials are stolen or leaked, the same incident must be reported to the IT team immediately.
- If the Project manager wishes to share the credentials with anyone, he/she must get permission in writing from a senior or appropriate person.
- The project manager or an allocated person will deal with the patient data and coordinate with the senior developer.
- If required, the project manager will take the help of a system administrator for transferring data from cloud workstation to a live server.
- Data transmission from cloud workstation to a live server must happen through SFTP, SSH, or HTTPS.
- Downloading patient data related documents on personal systems is not allowed and if anyone is found doing so, appropriate personnel will take the action.
- Developers can not take mysql dump of any database on their personal, office workstation or on Jump server.
- Data received as a JIRA request or an email must not be sent to anyone in the form of (but not limited to) email, chat, or simple text.

PHI Data Transfer:

PHI Data in excel sheets, PDFs,  SQL files and Simple Text can be transferred using below methods only,

- Email
- Dropbox
- Gdrive
- Pendrive - Use office Pendrive only
- JIRA Request

Above are the only PHI data transfer methods approved by Plus91.

# Report Abuse & Escalation Process

Immediately report any of the following to IT Team,

- Any user violating the server or data policy.
- Found any suspected or actual security breaches on the server.
- Suspected or actual weaknesses in the safeguards protecting Servers or Data.
- Found unauthorized third party service or software running on the server or on workstation.

Below are a few common incidents and how to escalate them with the appropriate team/personal.

| **Incident Type** | **Action to be taken** |
|---|---|
| Server not accessible or Live URL not working | Take a screenshot of the error message and with the server information, report it to the IT team |
| File Permission issue | Take a screenshot of the error message and with the server information, report it to the IT team |
| Found malicious code on Server | Report it to your manager and IT team. |
| Found suspicious activity on Server | Report it to your manager and IT team. |
| Client's live URL redirecting to suspicious URL/Location | Report it to your manager and IT team. |
| Error in establishing a database connection | Take a screenshot of the error message and with the server information, report it to the IT team |
| "500 Internal server error" on Browser | Report it to your manager and IT team. |
| Connection Error in Remote Desktop Connection | Take a screenshot of the error message and with the server information, report it to the IT team |
| Installation of new service or software | Contact the IT team. |

**Consequences:**

If anyone is found violating the policy, the action will be taken according to the Sanction Policy mentioned in the Plus91 IT and DATA Security Policies.

# Appendix A – Approved Softwares

| | |
|---|---|
| **Remote Connection tools** | AnyDesk |
| | TeamViewer |
| | Remmina |
| | PAC |
| **Browsers** | Google Chrome |
| | Safari |
| | Firefox |
| | Brave |
| **Testing tools** | Eclipse |
| | Selenium |
| **Development tools** | Visual Studio Code |
| | Sublime -Text |
| | MySQL Workbench |
| | SQLyog |

| | |
|---|---|
| | Git |
| | Postman |
| **Communication tools** | Zoom |
| | Slack |
| | Microsoft Teams |
| | Google Meet |
| **Finance & other Tools** | Microsoft Office |
| | VLC media player |
| | XPaint |
| | Libre Office |
| | Tally Solutions |