Document Identification

Document	Procedure for preparing Workstations and Printers in the COMPANY Computing Park
Areas involved	Security Division; IT Support Division; IT Networking Division.
Objective	Establish the standard configurations for workstations and printers in the COMPANY's Computing Park.
Reference	The standardization of workstations in the COMPANY's Computing Park.

Version and Revision Control

Document	Version	Date	Responsibles	Reviewers
Initial Action	1.1	July, 21, 2022	@brazilianscriptguy	All of You
Approval	2.2	July, 21, 2023	@brazilianscriptguy	All of You
Last Update	**8.8**	**March, 21, 2024**	@brazilianscriptguy	All of You

Document Classification

CONFIDENTIAL	For internal use only regarding institutional workstations configurations of the COMPANY. Access restricted to those responsible for workstation configurations.

Justifications

STRATEGIC OBJECTIVES **(ISO/IEC 20000 International Standard for IT Service Management)**	Improve Service Quality; Enhance Customer Satisfaction; Increase Operational Efficiency; Ensure Service Continuity; Drive Continuous Improvement; Enhance Risk Management; Foster IT Governance;

Summary

Unit I – Premises for the execution of the ITSM-Templates standard

1. The procedures must follow the order of this Check-List Document, and subsequent steps should not be executed without confirming the compliance of the previous steps:

a) Deployment of the standard ITSM O.S. image on the workstation, defining the default local administrator password;

b) Confirm that you have credentials with a profile to join workstations to the Domain;

c) When cloning the operating system, considering that the security identifiers of each operating system must be unique (SIDs), verify if the clone followed the **`sysprep`** standard, as this action is necessary to avoid duplicate identifiers on the Network;

d) Prior submission to the Security Division of the list of workstation and printer accounts to be created in the AD object structure, as well as the MAC addresses of the Printers and workstations that for some reason need to have their IP address defined statically;

e) Having knowledge of the credentials for updating/configuration/removal of Corporate AntiVirus and administrator credentials for Printers configs;

f) Prior communication to the IT Networking Division about the need for VLAN changes in the unit where you are performing the migration;

g) Use the updated version of the ITSM-Templates configuration folder and make use of the latest version of this Check-list;

h) Having standardized names for workstations and printers of the Unit to be migrated, you must consulting the IT Service Desk Manager;

i) Errors and impediments detected beforehand or during the process must be recorded and forwarded via Service Desk for resolution by the responsible support level;

j) The list with the names of Workstations and Printers must be sent (preferably by email) in advance to the User and Services Management Section, which must create the accounts in the Domain and confirm to the requesting Unit;

k) Naming errors of accounts detected during the workstation preparation process must be reported to the responsible section for immediate correction;

l) Reports of non-compliance with the definitions of this document must be sent weekly to the all IT Support Division Chiefs and to the IT Service Desk Division Chief and monthly to the Chief Information Officer;

m) Confirm whether the first stage of this process, which is the deployment of the standard ITSM image on the workstation, was completed, or request information from the IT Support Division Chief;

n) Confirm with the IT Support Division Chief that the cloning of the operating systems followed the premise that the security identifiers of each operating system (SIDs) are unique. This action is necessary to avoid duplicate security identifiers on the Network;

o) Confirm that the location where all setups and homologated configuration files are stored is the network share provided by the Security Division: …**\DML\IT-Support-Division** which contains all software **(DML Definitive Media Library)**;

p) Confirm with the IT Support Division Chief, about the submission of the following to the Security Division: Standard Unit Migration Form; standard configurations of the MAC addresses of the Printers and the MAC address of the biometric point workstation;

q) Confirm with the IT Support Division Chief, about the configurations and changes of Switches and VLANs in the unit where you are performing the migration, by the IT Networking Division;

r) Confirm with the IT Support Division Chief, about the configurations or adaptations of: DHCP Scope; Inclusion of VLAN in DNS; Inclusion of VLANs in Sites and Services and, creation of OU structures in AD;

s) Confirm with the IT Support Division Chief that you have copied the updated version of the ITSM-Templates configuration folder to your removable media and that you have the latest version of the Manual Check-List to apply ITSM-Templates on Windows 10x11 Workstations;

t) Confirm that in case of doubts, or the occurrence of errors or incidents, that are beyond your management or knowledge scope, you consult the IT Support Division Chief, for clarification or referral to the appropriate support level;

u) Commit to executing the following procedures, as they guarantee the adherence of the workstation operating system to the policies in the Domain authentication server and Domain Forest;

v) Scripts must be executed, with the use and guidance present in this Check-list Manual, obeying the order contained in each of the chapters and in the same sequence as presented here in the Check-list, as this ensures adherence and flow of the execution order of the configurations;

w) All functionalities, commands, and functions executed in this Check-list are resources present in the Windows operating system, without the intervention of other commands or external software that are not standard for Microsoft operating systems;

x) Level 01 Support teams are the operators and executors of the Check-list, and therefore, with the aim of maturing and ensuring compliance in the execution and communication of incidents in the execution of the operations described here, they must inform the IT Support Division Chief of the possibilities of changes in the scripts, and the Coordinators must communicate via administrative process to the Security Division;

y) Below is the detail of each folder and its contents in the **\ITSM-Templates** directory, and it informs that the function of each script is described in Unit III and Unit IV of this Check-list.

- **Certificates:** Folder containing COMPANY certificates that need to be installed during the initial workstation setup.

    - **ADCS-Server:** Folder containing the ADCS (Active Directory Certificate Services) certificate for COMPANY.

    - **RDS-Server:** Folder containing the RDS (Remote Desktop Services) certificate for COMPANY.

    - **WSUS-Server:** Folder containing the WSUS (Windows Server Update Services) certificate for COMPANY.

- **CustomImages:** Folder containing standardized COMPANY images for local user profile and desktop environment.

- **MainDocs:** Folder containing original and editable files of this ITSM-Templates Manual and the standard operating system figure template.
    - **Check-ListOrigin:** Folder containing the original and editable file of this Check-List.

    - **DefaultUsersAccountImages:** Folder containing institutional image files for user profiles. Also includes the hosts file containing protections against malicious sites, based on the company's Safer-Networking Ltd. blacklist. These could be replaced when the workstation joins the Domain and is protected by institutional antivirus and firewall.

- **ModifyReg**: Folder containing initial execution script folders.
    - **AllGeneralConfigs:** Folder containing general configuration scripts.

    - **DefaultBackground:** Folder containing desktop and logon screen configuration scripts.
        - **DesktopScreen:** Folder containing scripts affecting desktop environment images.
        - **LogonScreen:** Folder containing scripts affecting logon screen environment images.

    - **UserDesktopFolders:** Contains folders to be copied to each user's screen upon logging into the workstation, containing institutional shortcuts and links.
    - **UserDesktopTheme:** Contains scripts to apply the COMPANY institutional theme, changing default images, and scripts configuring the Windows environment for classic desktop use.

- **PostIngress:** Folder containing scripts to be executed after the workstation joins the domain.

- **ScriptsAdditionalSupport:** Folder containing additional support scripts, according to configuration inconsistencies already identified by IT Service Support Division.

    - **ActivateAdminShare:** Folder with script to activate administrative shares; RDP and download Windows Firewall.

    - **DiskVolumes:** Folder with script to locally rename disk volumes C: and D:.

    - **Export-Custom-Themes:** Folder with script to exports the custom themes files.

    - **GetSID:** Folder with Microsoft Internals application to identify the SID Security Identifier of the operating system.

    - **LegacyIngress:** Folder with script to allow legacy operating system workstations to join new domains.

    - **ResetGPOs:** Folder with script to reset all workstation GPOs and initiate a new synchronization.

    - **UnjoinDomain:** Folder with script to unjoin workstations from the domain and clear data from the old domain.

    - **WorkStationConfigReport:** Folder with script to generate configuration reports for each workstation and record them in a spreadsheet.

    - **WorkstationTimeSync:** Folder with script to synchronize workstation time, date, and time zone.

- **UniqueScripts:** Folder containing the 02 unified scripts for executing .REG registry configurations and configurations via .VBS scripts.

z) Reinforcing that the function of each workstation preparation script and the execution order are described in Unit III and Unit IV of this Check-List.

Unit II – Workstation Preparation and Update

1. Proceed with the customization of the operating system, known as `Out-of-box experience (OOBE)`, using the `sysprep` command settings and specifying an initial account to log into the operating system:

   a) Remove any other accounts with `Administrator` profile and enable the built-in Administrator account, set the new default password, use the command: `netplwiz` to ensure there is only one account with administrative privileges;

   b) Remove all local printers from the workstation, except: `Print to PDF`;

   c) Enable Network Properties settings (IP address and DNS), so that the workstation fetches network `settings automatically via DHCP`, and `verify/enable the IPv6 protocol`;

Note: In case of issues with obtaining an IP address via DHCP, reset the network environment settings: `C:\ITSM-Templates\ModifyReg\AllGeneralConfigs\`

- `Renew-all-IP-Connections.vbs`, renews TCP/IP connections;

Another solution is to, in `Device Manager`, remove the network adapter and choose to uninstall the network adapter driver, then restart the workstation.

2. Assess the need to run `WSUS-Offline Updater Tool,` checking which folder corresponds to the workstation's operating system version (Windows 7 and Windows Vista have no updates and should be discontinued in COMPANY).

3. If there is a need to run the `offline update`, follow the procedures below:

   a) On the `DML network share`, run the update application in the folder: (`\WSUS_Offline\client\UpdateInstaller.exe`) or via the media used for operating system updates;

   b) Check all installation options in the `Updating – Installation section` and do not check any options in the `Control section`;

   c) Restart the operating system when prompted with the message: `Installation successful. Please reboot your system`. and continue until there are no more pending updates, then restart the system and confirm in Control Panel if there are any pending updates.

Unit III – Standardize the Workstation for AD Domain Join

1. Now, connected with the local `Administrator` account of the workstation, emphasizing that only for workstations with Windows 10 and Windows 11 Operating Systems, where 02 scripts will be executed gathering the total configuration of the workstation environment:

   a) Copy the entire folder: `ITSM-Templates` to the root folder of the `C:\` drive of the workstation being configured;
   b) Open the folder `C:\ITSM-Templates\UniqueScripts\`;
   c) Run the Script for standardized desktop, themes, folders, for all versions of MS-Windows:

   • `ITSM-DefaultVBSING.vbs` (Note: run with right-click and choose: `Run with command prompt`.)

   This Script gathers 10 (ten) configurations, which are:

   1. `Disable-Windows-Firewall.vbs` – disables Windows Firewall;
   2. `Grant-Full-Access-Legacy-App.vbs` – Granting execution permissions in the root folder of your legacy application
   3. `Renew-all-IP-Connections.vbs` – renews TCP/IP connections;
   4. `All-Certificates-Install.vbs` – installs All your certificates;
   5. `WSUS-Clean-SID.vbs` – cleans previous WSUS connections;
   6. `CopyDefaultFolders.vbs` – copies default desktop folders and XML profile of desktop appearance and start button;
   7. `CopyHosts.vbs` – protects network connections before AV installation;
   8. `CopyLogonBackground.vbs` – copies standardized lock screen images;
   9. `CopyUserLogo.vbs` – copies standardized user profile images;
   10. `CopyWallPaperDefault.vbs` – copies standardized desktop wallpapers;

   Here extra attention is needed because as all 10 (ten) configurations are encapsulated in a single script, error messages must be observed for each step to be executed and, afterwards, the executor of the configurations will need to know exactly which configurations were made, and also to ensure that the results comply with the `ITSM-Templates` standard.

   d) Run the script for registry settings, standardized for all versions of MS-Windows:

   • `ITSM-ModifyREGING.vbs` (Note: run with right-click and choose: run with command prompt.)

   This Script gathers 10 (ten) configurations, which are:

   1. `AddStartPageADM.reg` – configure browser homepage;
   2. `DisableUAC-LUA.reg` – disable UAC;
   3. `Enable-AutoShareAdmin.reg` – enable administrative sharing;
   4. `Register-Owner.reg` – customize COMPANY data in Windows license;
   5. `WSUS-App-Intranet.reg` – point to corporate WSUS;
   6. `DesktopCurrent.reg` – configure graphical appearance of the OS – current user;

7. `DesktopDefault.reg` – configure graphical appearance of the OS – default user;
8. `EnableCustomLogonBackgrounds.reg` – customize wallpapers;
9. `Domain-Ingress-Win10x11.reg` – protect domain shares;
10. `ITSM-Templates.deskthemepack` – configure desktop theme;

Therefore, it is of great importance that the executor of the configuration procedures is attentive to the configurations being performed and ensures that the results comply with the `ITSM-Templates` standard.

Note: Check in the folder `C:\ITSM-Logs` if the script execution generated any error logs:

- `ITSM-DefaultVBSING.log`
- `ITSM-ModifyREGING.log`

In cases where errors occur that cannot be resolved immediately, report them to the appropriate support level through the Company Help Desk Tool.

Unit IV – Institutionalize the MS-Windows Workstations

Note: To ensure standardization in the information of each workstation and to allow IT Monitoring and Asset Management Software (CMDB) to correctly identify each workstation on the network, it is necessary to standardize the workstation identification settings.

Therefore, follow all the procedures described below, and in case of doubts or issues, always consult the IT Support Division Chief.

1. In the `Control Panel\Module\Network` and `Internet\Network Connections`, rename the active network connection to a name that reflects the configuration building: HQBNet; NYCNet; LAXNet, MCONet, ORDNet, DFWNet, DENNet, etc., according to the naming standard of the Headquarters and Branches (Annex – Unit VIII).

2. Standardize the `workstation name`; the `volume name` of the hard `disks C:` and `D:` and the `computer description`:

a) Workstation name, Example: `HQBITSERVC11704`; `NYCSALESOP07706`, consult the Host Naming Table with the IT Support Division Chief and in the Annex – Unit VIII, in this Check-List;

b) Volume label name of the `C:` drive: `HQBITSERVC11704` (same as workstation name);

c) Confirm that the volume label names of the drives:

- `C:` is the same as the workstation hostname and;
- the volume of the `D:` drive is: `Personal-Files`

d) Align the computer description according to the unit to which the workstation belongs, example: `Workstation – ITSERVICE`, or `Workstation – SALES OPS`

Note 1: The workstation hostname is composed of the: `equipment type designation letter, branch abbreviation, and equipment asset number`. For example, `HQBITSERVC11704` represents a workstation in the Headquarters Building, belonging to the IT Service Division, with an asset number of 11704. All workstation names must be within 15 characters.

And, if the second partition of the disk is not defined as the letter `D:`, perform the procedures for this change.

Example: `HQBITSERVC11704`; `NYCSALESOP07706`. Verify and confirm with the IT Support Division Chief this information, including for other hosts such as Notebooks, Printers, Multifunctionals, Scanners. In accordance with the naming standard for hosts and Organizational Units (in Annex – Unit VIII, in this Check-List).

Note 2: Verify all workstations and other hosts that require static IP addresses. Provide the MAC address of each workstation/host to the Security Division to grant the workstation's IP address via IP reservation. Additionally, inform the IT Support Division Chief of the need for static configuration.

Unit V – Setting up Printers and Multifunction Printers (MFP)

NOTE: Printers and Multifunction Printers (MFP) are also Active Directory Domain Objects and require specific configurations and firmware updates to join the Domain structure.

a) Force DHCP configuration acquisition on printers via the printer's physical panel;

b) Access the printer settings using the Embedded Web Server environment of each printer. Access through the assigned IP address;

c) Update the printer firmware;

d) Customize the printer's Administrator credentials (SNMP default credentials, verify with Security Division and IT Networking Division about the standard);

e) Configure the hostname following the standard naming convention for hosts and Organizational Units;

f) Disable all printer advertising protocols and disable printer Wi-Fi settings, except for the following protocols, which should remain active:

- `RAW TCP/IP on Port 9100/SMB, and`
- `HTTP on Port 80`

g) Configure SNMPv3 and SNMPv2 credentials (in agreement with Security Division and IT Networking Division);

h) Configure the date and time service to synchronize via the NTP Server: `ntp1.company.com`;

i) Enable the internal RAM module and printer storage disk;

j) Configure the login account for multifunction printer scanning on the network;

k) Configure IP address acquisition via DHCP, informing the Security Division of the printer's MAC address for IP address reservation; Blocked and Allowed Protocols;

l) Identify the friendly name that the printer will display in the user's printer list.

Example:
`PRN-ITSERVICE-4020ND`; `PRN-SALESOPS-L14510`; `PRN-ENGINEERING-HPCOLOR`: These friendly name details need to be synchronized with the Security Division and incorporated into the IT Support Division's service report to streamline identification across all support levels.

Unit VI – Joining MS-Windows Workstations to the to the AD Domain

NOTE: The workstation's joining to the Domain Controller Server can only occur after all previous procedures have been performed and verified.

Do not proceed to the next steps without first validating all previous procedures and configurations, as this compromises the validation of the workstation's operating system and consequently all work executed up to this point.

1. In `System Properties`, choose the option to `Change`, and then provide the computer name and the Domain to which the workstation will be a member.

2. Confirm the workstation's enrollment with the domain ingress credential provided by the IT Service Support Chief.

3. Confirm that the workstation restarts after joining the Domain.

4. After the workstation restarts, execute the workstation's DNS registration to register the new hostname and new Domain information:

In the folder `C:\ITSM-Templates\PostIngress\`

• `ITSM-NewDNSRegistering.vbs` – register the new DNS data for the workstation; (Note: right-click and choose: Run with command prompt.)

This script will register the new workstation data in the DNS Servers of the COMPANY AD Forest structure.

5. After joining the workstation to the domain, and for all workstations, even if they are used within COMPANY or outside COMPANY's network, the following procedures must be performed, with 03 logons by each user, logoff, and reboot, to enforce the network scenario, domain settings, and user profile registration on the workstation to be used outside COMPANY's network, including workstations that remain within COMPANY's network:

In the folder `C:\ITSM-Templates\PostIngress\`

• `ITSM-ProfileImprinting.vbs` – register the user's profile on the workstation; (Note: right-click and choose: Run with command prompt.)

This script, after the user's 03 logons, will register the user's Domain profile on the workstation so that the user can use the workstation outside COMPANY's network environment.

It's important for the settings executor to confirm if the configurations were performed and to ensure that the results are in accordance with the `ITSM-Templates` standard.

6. After executing the above procedures, the configurations need to be verified within the User's workstation profile, as follows:

a) Check if the `T:\ network drive` is mapped in Windows Explorer and if its contents correspond to the user's allocation profile;

b) Verify if the `D:\ drive` is the drive where the user's profile is stored;

c) Verify if the Printer was mapped to the user's profile, according to the friendly name previously defined;

d) Open all browsers and access different portals, checking for correct access and assembly of the portal;

e) Check if the following log files were created in the `C:\ITSM-Logs` folder for the execution of the Scripts in this Check-list, regarding the workstation configurations:

- `ITSM-NewDNSRegistering.log`
- `ITSM-ProfileImprinting.log`
- `ITSM-DefaultVBSING.log`
- `ITSM-ModifyREGING.log`

NOTE: The interaction of scripts via confirmation messages with the executor is necessary so that the executor understands the waiting time and transition between one execution and another, and interactions that take less time are omitted from the interaction windows.

Unit VII – Join MacOS Workstation to the AD Domain

1. **Procedures for joining MacOS workstations to the AD Domain:**
   a) Synchronize date/time and time zone (automatically);
   b) Create **Administrator** user and set default password;
   c) Log in as **Administrator** and remove all other users;

2. **Via CMD/Terminal, access:**
   a) `sudo nano /etc/ntp.conf`
   b) `server 10.10.0.100` (leave only this line)
   c) Save and restart the workstation

3. **In System Preferences:**
   a) Under `SHARING`, enter the asset's hostname;
   b) Under `Users & Groups`:
   c) Unlock the padlock for editing (Mac `Administrator` password);
   d) Change startup method;
   e) Click on `Login Options`;
   f) Under `server`: `YOUR-FQDN-DOMAIN-NAME` (OK and Domain user that can ingress workstations);
   g) On the same screen, click `Open Directory Utility`;
   h) In `Directory Utility`, click on `Active Directory and in its options`, check `"Create mobile account at login"` and uncheck `"Require confirmation before creating a mobile account"` ->> to allow users to log in without being in the domain environment

4. **For Network Drive Mapping:**
   a) Under the logged-in user, access the drop-down menu and click on: `Connect to Server`
   b) Enter in the box: `smb://file-server-fqdn-name` and select the mapping

Unit VIII – Attachments Host Naming Standard Table

STANDARD HOST NAMING FOR HEADQUARTERS AND BRANCHES

For example, "NEW YORK BRANCH" would be:

Workstations Desktops

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
N	Y	C	D											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Workstations Notebooks

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
N	Y	C	N											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Printers and Multifunction printers (MFP) (Printers)

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
N	Y	C	P											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Network Scanners (not attached to multifuncion devices)

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
N	Y	C	S											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Identification for the naming of hosts, sites, and services:

Headquarters Building - HQB
Atlanta - ATL
Boston - BOS
Charlotte - CLT
Chicago - ORD
Dallas - DFW
Denver - DEN
Detroit - DTW
Houston - HOU
Las Vegas - LAS
Los Angeles - LAX
Miami - MIA
Minneapolis - MSP
New York City - NYC
Orlando - MCO
Philadelphia - PHL
Phoenix - PHX
San Diego - SAN
San Francisco - SFO
Seattle - SEA
Washington, D.C. - DCA
Austin - AUS
Nashville - BNA
Portland - PDX
San Antonio - SAT