Technician Name:		Date:
Location:		Incident Number
POC:		

UPS #1	
Is the UPS on-site currently in use?	
Brand	
Model	
Rating	
Plug Density	
Outlet Occupancy	
Outlet Vacancy	
IP Manufacturer Name	
Open Socket Count	
Is this UPS network capable?	
Is the UPS currently connected to the network?	
Were there any UPSs offline/unplugged? (Yes/No)	
If 'Yes', what port did the UPS get plugged into (port 48 or another)	
Does it have a NIC	
Has local management expressed the need of a UPS replacement at this location?	
Expiration Tag (if available)	
Devices Currently Pluged into the UPS	
Device #1 (including make and model)	
Device #2 (including make and model)	
Device #3 (including make and model)	
Device #4 (including make and model)	
Device #5 (including make and model)	

UPS #2
Is the UPS on-site currently in use?
Brand
Model
Rating
Plug Density
Outlet Occupancy
Outlet Vacancy
IP Manufacturer Name
Open Socket Count
Is this UPS network capable?
Is the UPS currently connected to the network?
Were there any UPSs offline/unplugged? (Yes/No)
If 'Yes', what port did the UPS get plugged into (port 48 or another)
Does it have a NIC
Has local management expressed the need of a UPS replacement at this location?
Expiration Tag (if available)
Devices Currently Pluged in
Device #1 (including make and model)
Device #2 (including make and model)
Device #3 (including make and model)
Device #4 (including make and model)
Device #5 (including make and model)

Circuit Information			
Existing Circuit IDs	Circuit Location (MDF, IDF1, IDF2, etc)	Circuit Type (Fiber, Cable, etc)	Carrier

Cellular Coverage	

Using a cellphone with Verizon or AT&T as carrier, determine if there is optimal cellular coverage in the IT closets (MDF/IDF)		Cable Category
AT&T Coverage		Is the cable in good condition or does it need to be replaced?
Verizon Coverage		Are all cable runs terminated to a patch panel?

MDF/IDF High Resolu

MDF

UPS #1

Make
Model
Serial #

Router

Sensitivity: Internal

TECH AMERICAS Service. Support. Solved.	
Site Name:	**UPS**
Brand:	
Model:	
Description of Check List	**Y/N**
-Is the UPS Working Properly (Any errors reported by APC network Card?)?	
-Check Condition of the UPS	
-Are proper indicator lights on	
-Is the unit wired properly	
-Is there evidence of pest infestation	
-It has physical damage	
Charge Load	**Provide information from the UPS**
-Runtime	
-Input Voltage	
-Output Voltage	
-Battery Capacity %	
-Battery Voltage	
-Load Power % in Watts	
	Y/N
Does this UPS needs to be replaced?	

windstream

Check List

Comments
Comments
Comments

TECH AMERICAS
Service. Support. Solved.

Endpoint Security Policy

Last Review: January 2021
Next Review: June 2021
Effective Date: January 1st, 2021

Presented by:

Tech Americas USA

Contents

Purpose

The purpose of this policy is to regulate protection of the customer network when accessed by Endpoint equipment such as laptops, tablets, and mobile devices. It is designed to protect our employees, customers and other partners from harm caused by the misuse of IT systems and data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Definitions

"Users" are everyone who has access to any of the Customer IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

"Systems" means all IT equipment that connects to a corporate network or accesses corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Objective

The objective is to reduce the risk of security breaches that could result from the connection and use of Endpoint devices. This policy seeks to limit security threats by:

- Ensuring Users are aware of the requirements and restrictions around Endpoint devices.
- Enabling protective measures and controls to manage Endpoint security and software compliance risks.

Audience

Everyone who works at Tech Americas USA or anyone performing work on behalf of Tech Americas USA including contractors, consultants and volunteers are subject to this policy and responsible for the security of customer IT systems and the data on them. As such, everyone must ensure they adhere to the guidelines in this policy at all times.

Scope

This policy covers all Endpoint devices connected to any customer network.

Policy

This Audience is responsible for ensuring that:

Information Security

- All care is taken to prevent unintended exposure, modification, or removal of private, copyright, or confidential information as a result of leaving this information on the screen or desk, or exposed in such a way that it can be viewed or accessed by an unauthorized individual. This includes information stored on portable storage media or hard copy.
- Any private, sensitive, or confidential information that is stored on such an Endpoint device has the appropriate security controls to restrict and prevent retrieval or intercept by an unauthorized third-party.

End Point Software

All software contains security vulnerabilities, and software vendors are constantly supplying updates (patches) to address these vulnerabilities when they are identified.

- Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical to do so, i.e.:
  - Critical security patches are applied within 1 week of them being released by vendors
  - Important security patches are applied within 2 weeks of them being released by vendors.
  - Endpoint systems must be restarted following installation, to ensure security patches have been fully installed.
  - Where possible, it is recommended that Endpoint devices are set to auto-update their security patch levels, and restart if necessary to complete the installation.

Computer and Data Security

If data on the Customer systems is classified as confidential users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Customer system any information that is designated as confidential, or that they should reasonably regard as being confidential to the Customer except where explicitly authorized to do so in the performance of their regular duties.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices.

Multiple layers of security practices should be utilized for devices connected to the Customer systems. These layers include firewalls, up-to-date anti-virus software, current software security patches and spyware removal and detection software.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the Customer systems by whatever means.

All devices being connected to Customer systems should be for professional use and not contain personal documents or any have any content related to activities that are inappropriate for the Customer to be associated with and/or are detrimental to the company's reputation, including pornography, gambling, inciting hate, bullying and harassment.

Enforcement

Tech Americas USA will not tolerate any misuse of customer systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, Users should be aware that consequences may include the termination of their employment.

Use of any of the customer resources for any illegal activity will usually be grounds for summary dismissal, and Tech Americas will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Acceptance and Authorization

Performing service work by accepting a work order from Tech Americas USA implies acceptance of this policy. I have read and understand and agree to abide by its terms and conditions. I understand that violation of the use and provisions stated in the policy may result in limitations, suspension or dismissal, and/or disciplinary actions by Tech Americas USA or by legal authorities.