THE TJX COMPANIES, INC.

Marshalls **T·J·maxx** **HomeGoods**

Remodel Vendor Site Survey

CHAIN:

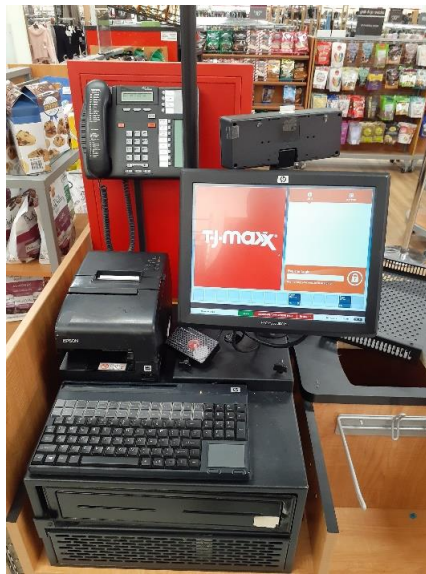STORE #:

MANAGER NAME:

DATE OF SURVEY: @ 7:30 AM

VENDOR COMPLETING SURVEY: Fujitsu

Take Photos as shown on Pages 3 – 5
Complete all questions on Pages 6 - 10

Take only the following Pictures:

Complete Frontline from the customers view

Register Closest to the front door

Call Forwarding Main Display
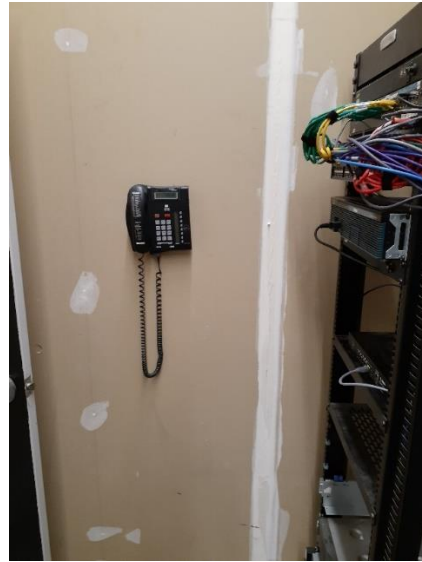
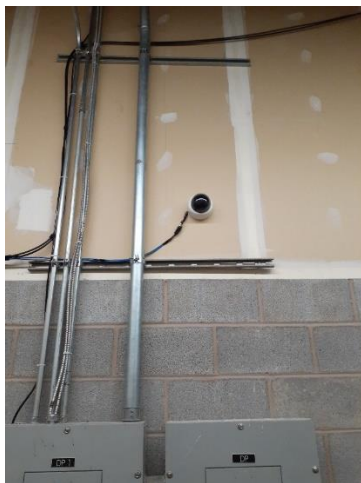**Frontline IDF Cabinet (if applicable)**

Jewelry Register (if applicable)

Office IDF patch panel & switch

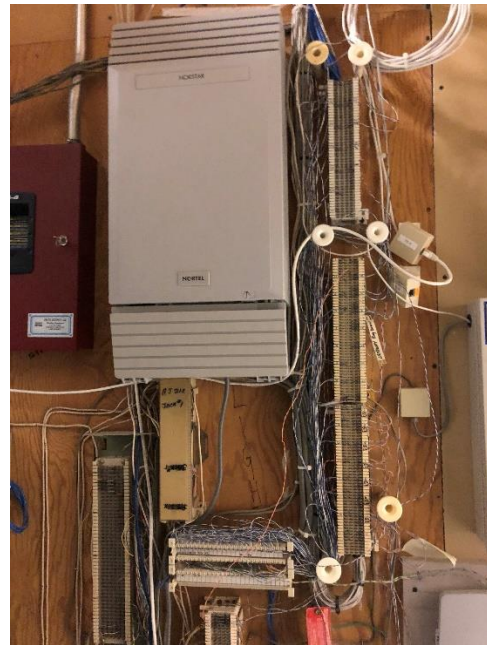**System Rack Full view**

System Room Telephone
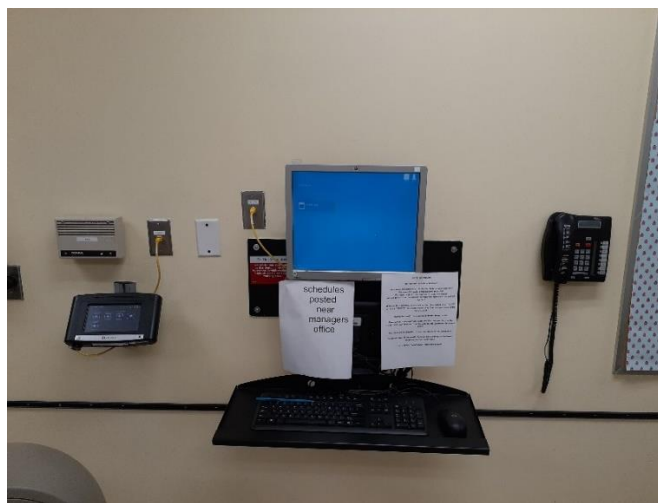

System Rack Camera

System Room door lock

Sound System
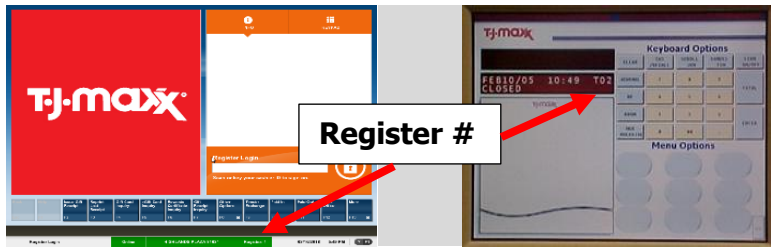

Telephone System

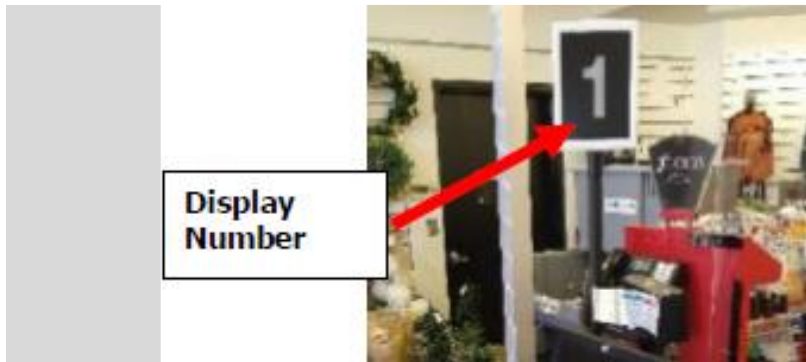**Lounge Time Clocks & Telephone**

Training Room (If applicable)

Frontline Checkout:

1. What is the total number of registers at the Frontline? _____

2. Document the Register # closest to the Front Door: REGISTER #: _____

Register #

3. Document the display # on the Register closest to the Front Door: REGISTER #: ___

Display Number

4. Does the store have a front line switch installed (Single Queue only)? Yes / No

Patch Panel

Power Strip

HP Switch

5. Does the store have a Second entrance? If yes, what is the total number of registers at that entrance? _____

6. What is the total number of Registers in the Layaway Dept.? ___

7. What is the total number of Registers in the Jewelry Dept.? ___

8. Circle which software is installed at this store?
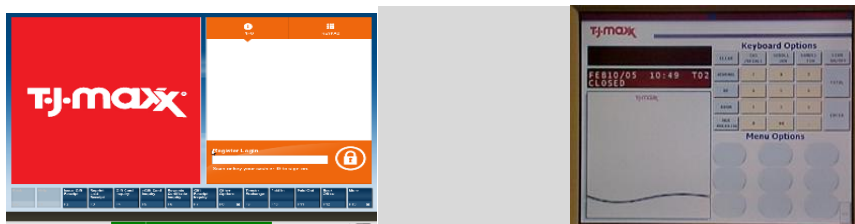
Are any Register Distributed? YES / NO
HP Distributed Register

Which Reg #'s? _____

Service Desk Telephone behind the Register Frontline. -

Does Telephone jack exist: Yes / No
Does Power Fail phone jack (PF1) exist: Yes / No
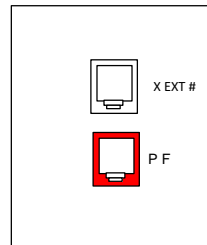
Sound System/Speakers

Sound System:

Please circle the sound system (if it is not pictured here, please make a note here of the manufacturer).
_____

TOA

VALCOM

Speakers:
Are the Store speakers Bose? Yes / No

Which Phone System does Store have? Circle One

KSU

BCM

Avaya

Where is the Phone system located? Electrical Room or System Room

Back Offices

Loss Prevention
Does the Loss Prevention office have speakers? Yes / No
Does the Loss Prevention office have a volume control on wall or speaker? Yes / No
Is there currently a phone installed in the Loss Prevention office? Yes / No
Is there a Camera Yes / No
Is there currently an IDF (Switch) installed in the LP for Cameras? Yes / No

Assistant Manager
Does the Assistant Managers office have speakers? Yes / No
Does the Assistant Managers office have a volume control? Yes / No
Is there currently 2 phones installed in the Assistant Managers office? Yes / No
Is there a Patch Panel & HP Switch in the Assistant Managers office? Yes / No
How Many HP Switches? _____
Is the patch panel & HP switch in a wall-mounted rack? Yes / No

Manager Office
Does the Managers office have speakers? Yes / No
Does the Managers office have a volume control? Yes / No
Is there a Patch Panel & HP Switch in the Assistant Managers office? Yes / No
How Many HP Switches? _____
Is the patch panel & HP switch in a wall-mounted rack? Yes / No

Cash Office
Does the Cash office have speakers? Yes / No
Does the Cash office have a volume control? Yes / No
Is there a Patch Panel & HP Switch in the Assistant Managers office? Yes / No
How Many HP Switches? _____
Is the patch panel & HP switch in a wall-mounted rack? Yes / No

Learning Center (If applicable)
Are thin clients currently installed in the Training room? Yes / No
Are data lines run to the Training room? Yes / No
Are Phones currently installed in the Training room? Yes / No
Does the Training Room have speakers? Yes / No
Does the Training Room have a volume control? Yes / No

Lounge
Does the Lounge have speakers? Yes / No
Does the Lounge have a volume control? Yes / No
Does the lounge have a 7208 or 1408 telephone mounted on the wall 54" from the floor near the time clock? Yes / No

Fitting Room
Does the Fitting Room have speakers? Yes / No
Does the Fitting Room have a volume control? Yes / No
Is a phone currently installed? Yes / No
Is the Fitting Room TV installed? Yes / No

EnGenius Durafon Wireless Telephone (HomeGoods only)

Which Wireless Telephones does the Store have? Circle One

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.