Table of Contents

First 5 Minutes
- Break in and change admin/root password
- Fill out system profile

First 20 Minutes
- Update services
- Configure firewall
- Backups + basic hardening (AV)

First Hour
- Further audits and hardening complete
- Centralized logging and HIDS

Initial Tasks

Breaking In

Windows

- Sticky keys
    - Press shift five times, an administrative command prompt should pop up. Enter command “net user Administrator *” and reset the password.
    - *If you are logged in but don’t have Admin:* reset the computer and boot into a command prompt by pressing F8 during boot and selecting the command prompt. Type “copy c:\windows\system32\sethc.exe c:\” (without quotes), then “copy /y c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe”. Reboot the computer, and follow the above directions to reset the Administrator password.
- Default passwords
    - [blank]
    - admin
    - password
    - changeme
    - letmein
    - ccdc
- Domain accounts (have Domain Admin give you an account to login)
- Passwords hidden on other systems?
- Services that log into box from other machines

Linux

- Single user mode
    - **BSD:** during boot, you’ll be prompted with a splash screen to enter multi/single user mode. Go to single user mode and change root/admin password. Note: it may be necessary to remount root partition so that you can write changes: “mount -a -o rw”, and then reset root password and reboot.
    - **Debian:** during boot, press shift to go to the Grub menu. Modify the boot commands by finding the line that begins with “linux#”, where the # is either 16 or 32. In that line there should be a “ro” which you should change to “rw” and finally somewhere in the line (it’s arbitrary where) add “init=/bin/bash” without quotations. Reset root password and reboot.

        - **Fedora:** Just like debian, except instead of “init=/bin/bash” add “init=/sysroot/bin/sh”. Reset root password and reboot.
- Default passwords
    - [blank]
    - toor
    - root
    - admin
    - password
    - changeme
    - letmein
    - ccdc
- SSH from other boxes that might have *authorized_keys*

Mac

- Single user mode
    - Hold command-S on startup
    - Run “mount -uw /”
    - For 10.7 and later (one command):
        - launchctl load /System/Library/LaunchDaemons/com.apple.opendirectoryd.plist
    - For 10.6 and before (one command):
        - launchctl load /System/Library/LaunchDaemons/com.apple.DirectoryServices.plist
    - Reset the password using “passwd <username>”
    - Then finally “reboot”
- First time setup
    - Hold command-S on startup
    - Run “mount -uw /”
    - Run “vm /var/db/.AppleSetupDone”
    - Then “reboot”
    - Create a new administrator account
    - Reset the password of the old account from the Users &

Palo Alto

- Reboot the router
- Press ‘m’ during boot to bring up the boot menu (or ‘maint’)
- Use the menu to revert to a known config or factory reset the router
- Reset IP address:
    - configure
    - set deviceconfig system ip-address <IP> netmask <netmask> default-gateway <gateway IP> dns-setting servers primary <DNS IP>
    - commit

Change Password

Linux: passwd <username>
Windows: net user <username> *

- Requires Administrative privileges

Update Services

- Run tcpdump[1]/Wireshark[2] for at least 5 minutes and determine how scoring is working then do the following if they won't affect scoring. If they will affect it, write them down and let the service lead know.
  - Make sure service administrators have changed passwords
  - Make sure general users don't have blank passwords and anonymous access is disabled
- Google your service version number with "exploit" after it (or check exploit-db.com)
- Make backups of your service files and configs
- Update service to latest version if possible
- Make sure service isn't running as root

[1] apt-get install tcpdump
[2] Wireshark: https://goo.gl/q55fWn

Firewall Configuration

Linux/IPTables

Do these in exact order. If you have questions, ask your firewall lead.

```
#Set to Deny All by default
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

#Allow ping
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

#Allow outbound DNS
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT

#Prevent DoS attack
iptables -A INPUT -p tcp --dport <port #> -m limit --limit 50/minute --limit-burst
    200 -j ACCEPT

#Allow connections to <port#> from outside to inside (ingress). Do once for each port.
iptables -A INPUT -p <tcp/udp> --dport <port #> -m state --state NEW,ESTABLISHED -j
    ACCEPT
iptables -A OUTPUT -p <tcp/udp> --sport <port #> -m state --state ESTABLISHED -j
    ACCEPT

#Allow connections to <port#> from inside to outside (egress). Do once for each port.
iptables -A OUTPUT -p <tcp/udp> --dport <port #> -m state --state NEW,ESTABLISHED -j
    ACCEPT
iptables -A INPUT -p <tcp/udp> --sport <port #> -m state --state ESTABLISHED -j ACCEPT

#To backup iptables rules:
iptables -L -nv --line-number
iptables-save > savedrules.txt

#To restore iptables rules from a backup:
iptables -F
iptables-restore < savedrules.txt
```

Windows

For every Windows Machine

Turn on Firewall:

Start menu

Windows Defender Security Center > Firewall and network projection

OR: System and Security > Windows Firewall

Windows Firewall: ON

Disable RDP:

1. In Control Panel, click System And Security, and then click System.

2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box to the Remote tab.

3. Select Don't Allow Connections To This Computer, and then click OK.

For Domain Controller

1. Open the Group Policy Management Console to Windows Firewall with Advanced Security.
2. Go to **Inbound Rules** and select **New Rule** then **Port** and then Next.
3. Make sure TCP is selected and type in 3389 into the Specified Local Port field and click Next.
4. Select **Block the Connection** and then next. Make sure all three are checked and press Next.
5. Name the rule "Block Remote Desktop" and then do it again under **Outbound Rules**.
6. Check the system profile sheet for outgoing ports and make specific outbound rules that **allow** these to be used.
7. Right click on **Windows Firewall With Advanced Security** and select **Properties**
8. Go to Domain Profile and select **Customize** near Settings. By "Display a notification:" change the rule to "Yes" (This will hopefully allow us to see if Red Team gets blocked or if we miss a rule.)
9. For each network location type (Domain, Private, Public), perform the following steps:
10.
    Click the tab that corresponds to the network location type.
    Change Firewall state to On (recommended).
    Change Inbound connections to Block (default).
    Change Outbound connections to block. **IF ANYTHING BECOMES UNABLE TO CONNECT, DISABLE THIS RULE IMMEDIATELY AND CHECK YOUR OUTBOUND PORTS!**
11. Select **Customize** near "Logging" and note the path. Open that and check it regularly.

DNS Logging:

1. Type **eventvwr.msc** at an elevated command prompt and press ENTER to open Event Viewer.
2. In Event Viewer, navigate to **Applications and Services Logs\Microsoft\Windows\DNS-Server**.
3. Right-click **DNS-Server**, point to **View**, and then click **Show Analytic and Debug Logs**. The **Analytical** log will be displayed.
4. Right-click **Analytical** and then click **Properties**.

5. Under **When maximum event log size is reached**, choose **Do not overwrite events (Clear logs manually)**, select the **Enable logging** checkbox, and click **OK** when you are asked if you want to enable this log.

By default, analytic logs are written to the file: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.etl. Use these analytics to monitor other services at will.

File Inventory and Backups

Backups/Snapshots

Snapshot once after initial profile and password change (get approval from manager first).
Every 2 hours do password protected zip backups of critical files, directories, or databases.

- Windows:
  - Download 7ZIP[3]
    Create archive, add password from password sheet.
  - Name like: hostname_folder--folder--file-name_time.tar.gz.team3
    Hostname_folder--folder--file-name_time.zip.team3
  - Store in C:\System\Zips
- Linux:
  - Install gzip if it isn't already installed
  - tar zcv - <directory> | gpg -c --cipher-algo aes256 -o <name>.tgz.gpg
    - Follow naming convention above for <name>
  - Store in /var/filestuff
  - To decrypt: gpg -o- <name>.tgz.gpg | tar zxvf -

Intellectual Property (IP) Handling

1. Find all file shares on the system. Look for files in common directories.
   - Linux: /root, /home/*, /tmp
   - Windows: C:\Users*

2. Run tcpdump or Wireshark for 5 minutes or use logging to see if files are accessed/scored.

3. If files are not being scored/checked, move all files on a system to a single directory and encrypt it.
   - Create backup (see instructions above)
   - Delete originals but only after making note of original location and verifying new copy. (if you haven't taken an original snapshot may want to do that too)

4. If files *are* being scored/checked, alert service lead.
   - Harden service/system as much as possible to mitigate risk
   - Prepare a list of hardening steps that you can't complete but would like to propose to white team.

[3] 7Zip: https://goo.gl/0oRcAy

Basic Hardening

Do not run as root/administrator. Create a normal user and elevate privileges when necessary.

Disable (don't delete) administrators not in use. Flag users with no passwords.

Windows

- Install EMET (https://goo.gl/iM0EZb)
- Restrict file shares/Harden SMB*
- FuzzySecurity System Profiler: https://goo.gl/5kY8Xp

Linux

- Restrict file shares
- Restrict SSH logins (prefer to use keys+passwords for everything)
- Enable SELinux/AppArmor (if you know how to handle them, else they can be scary)
- Lockdown Cronjobs (echo <username> >> /etc/cron.deny)
- Disable IPv6 if not in use
- Lock accounts (lock: passwd -l <username> unlock: passwd -u <user>)
- SysProf System Profiler: https://goo.gl/pVuJ7V
- Enforce stronger passwords:
    - /etc/pam.d/system-auth
    - /lib/security/$ISA/pam_cracklib.so retry=3 minlen=12 lcredit=-1 ucredit=-2 dcredit=-2 ocredit=-1

Advanced Hardening and Logging

OSSEC

Downloads: http://ossec.github.io/downloads.html

Agents:

- Linux: https://goo.gl/j7DFN6
- Windows: https://bintray.com/artifact/download/ossec/ossec-hids/ossec-agent-win32-2.8.3.exe
- Run ./install.sh. Import a key at the end from the server.
- tail /var/ossec/logs/ossec.log

Firewall:

Communication between the agent and server takes place over UDP port 1514, so you'll have to add a rule to iptables on both ends to allow traffic through that port.

First, temporarily remove the drop rule on both the agent and the server.

```
sudo iptables -D INPUT -j DROP
```

To add the rule to the OSSEC server, enter the following, using your OSSEC agent's IP.

```
iptables -A INPUT -p UDP --dport 1514 -s your_agent_ip -j ACCEPT
```

Then on the agent, enter the following, using your OSSEC server's IP.

```
iptables -A INPUT -p UDP --dport 1514 -s your_server_ip -j ACCEPT
```

Next, allow all outbound traffic through the firewall on both the agent and the server.

```
iptables -A OUTPUT -j ACCEPT
```

Finally, add the drop rule again to both.

```
sudo iptables -A INPUT -j DROP
```

Audit Linux

```
wget https://cisofy.com/files/lynis-2.4.6.tar.gz
tar xfvz lynis-<version>.tar.gz
./lynis audit system --quick
```

Update Kernel

- Ubuntu:
  - sudo apt-get update
  - sudo apt-get install linux-virtual
- Debian:
  - sudo apt-get update
  - For x64: sudo apt-get install linux-image-amd64 linux-headers-amd64
  - For x32: sudo apt-get install linux-image-686-pae linux-headers-686-pae
- Fedora/CentOS: sudo yum update kernel
- Reference the chart at the end of the playbook for more information on kernel versions

- Some language interpreters such as C/C++, Java, Perl, etc., can be exploited to escalate privileges, so it's best to remove compilers that aren't necessary (a webserver really doesn't need a C++ compiler installed).
    - apt-get purge <compiler>
    - yum remove <compiler>

Fail2Ban

https://linode.com/docs/security/using-fail2ban-for-security/

- Fail2Ban is a service that monitors connect attempts to other services (SSH, MySQL, Web) and limits the number of malformed/failed connections that might be indicative of a brute force attack
    - Instsall fail2ban:
        - yum install epel-release && yum install fail2ban
        - apt-get install fail2ban
    - Configure fail2ban:
        - In the jail.conf file, you can uncomment the specific services you want fail2ban to protect
        - **For CentOS:** you'll need to ensure in the jail.conf file that the "backend" option is set to "systemd"
        - You can add a whitelist for IPs with the option "ignoreip = <IP> <IP>"
        - Adjust bantime and maxretry to your likings

Audit Windows

powershell
Set-ExecutionPolicy Unrestricted -Scope Process;
Invoke-WebRequest -Uri 'https://github.com/iadgov/Secure-Host-Baseline/archive/master.zip' -OutFile 'C:\Users\Public\Secure-Host-Baseline-master.zip';
Unblock-File -Path 'C:\Users\Public\Secure-Host-Baseline-master.zip';
Add-Type -assembly "system.io.compression.filesystem";
[System.IO.Compression.ZipFile]::ExtractToDirectory('C:\Users\Public\Secure-Host-Baseline-master.zip', 'C:\Users\Public\');
Rename-Item -Path 'C:\Users\Public\Secure-Host-Baseline-Master' -NewName 'Secure-Host-Baseline';
Import-Module -Name 'C:\Users\Public\Secure-Host-Baseline\Scripts\GroupPolicy.psm1';
Invoke-WebRequest -Uri 'https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/telligent.evolution.components.attachments/01/4062/00/00/03/65/94/11/LGPO.zip' -OutFile 'C:\Users\Public\LGPO.zip';
[System.IO.Compression.ZipFile]::ExtractToDirectory('C:\Users\Public\LGPO.zip', 'C:\Users\Public\');
Remove-Item -Path 'C:\Users\Public\LGPO.pdf';
Invoke-ApplySecureHostBaseline -Path 'C:\Users\Public\Secure-Host-Baseline' -PolicyNames 'Adobe Reader','AppLocker','Certificates','Chrome','EMET','Internet Explorer','Office 2013','Office 2016','Windows','Windows Firewall' -ToolPath 'C:\Users\Public\lgpo.exe';
Import-Module -Name 'C:\Users\Public\Secure-Host-Baseline\Compliance\Scripts\Compliance.psm1';
Start-Transcript -Path 'C:\Users\Public\ComplianceReport.txt';
Test-Compliance -Path 'C:\Users\Public\Secure-Host-Baseline\Adobe

```
Reader\Compliance\AdobeReaderDC.audit' -Verbose;
Test-Compliance -Path 'C:\Users\Public\Secure-Host-Baseline\Chrome\Compliance\GoogleChrome.audit'
-Verbose;
Test-Compliance -Path 'C:\Users\Public\Secure-Host-Baseline\EMET\Compliance\EMET_5.5.audit'
-Verbose;
Test-Compliance -Path 'C:\Users\Public\Secure-Host-Baseline\Internet
Explorer\Compliance\InternetExplorer11.audit' -Verbose;
Test-Compliance -Path 'C:\Users\Public\Secure-Host-Baseline\Windows\Compliance\Windows10.audit'
-Verbose;
Test-Compliance -Path 'C:\Users\Public\Secure-Host-Baseline\Windows
Firewall\Compliance\WindowsFirewall.audit' -Verbose;
Stop-Transcript;
powershell "Select-String -Path 'C:\Users\Public\ComplianceReport.txt' -Pattern 'FAILED' | Foreach
{$_.Line} | Write-Host -foregroundcolor Red -backgroundcolor Black";
Remove-Item -Path 'C:\Users\Public\LGPO.zip';
Remove-Item -Path 'C:\Users\Public\LGPO.exe';
Remove-Item -Path 'C:\Users\Public\Secure-Host-Baseline-master.zip';
Remove-Item -Path 'C:\Users\Public\Secure-Host-Baseline' -Recurse;
powershell "echo 'ComplianceReport.txt Generated in C:\Users\Public' | Write-Host -foregroundcolor Blue
-backgroundcolor White";
```

Injects

General

Cut yourself off 10 minutes before and type a response.
5 minutes before have it reviewed by a returner or the manager.
Always be professional. Start with “CIO:” or “CEO:”. End with “Respectfully, IT Team x”.

Injects that **were not** completed

- Explain any results that were completed. Explain what portions were not completed.
    - If they are *actually* about to be finalized, then give a time estimate of verified completion. For example
        - “While attempting to complete a full risk assessment of the network, we set up OpenVAS and nmap as requested. OpenVAS scans are still in progress, however preliminary results from nmap are attached. OpenVAS results should be completed in 10 minutes, and we would be happy to provide them as they are available.”
    - If you don’t know for sure a completion time, don’t bother. For example
        - “While performing a full risk assessment of the network, we attempted to use OpenVAS and nmap as requested. Unfortunately we were unable to complete OpenVAS in the time allotted, however nmap results are attached.”

Injects that **were** completed

- Restate the task (concisely) and that it was completed. Provide any information they may have requested or need to verify it is working. For example:
    - “As requested, we have set up a chat server for all employees. It is available at 10.1.2.3 and users daniel and engels may log in with their normal Windows passwords. Respectfully, IT Team 3”
    - “As requested, we have performed a risk analysis of our company’s network. Please find attached a report detailing our findings and recommendations. Respectfully, IT Team 3”
    - “As requested, we have drafted an Acceptable Use policy for the organization. Please find our recommendations attached for review and approval by Legal. Respectfully, IT Team 3”

Policies

- **Must be reviewed by a returning member 10-15 minutes before submission.**
- Write something custom. You can use SANS/others as references. Don't copy/paste.
- Better to be concise/hit all points than be pages and not directly address concerns.
- Include: Purpose, Affected Parties, Policy Guidelines/Restrictions, Exceptions (if applicable), Disciplinary Actions if Broken, Signature for Employee
- **Incident Reporting Policy:** https://goo.gl/H5YYEU

BYOD Policy

Example: Smartphone use is a privilege given to employees of *Planet Express Trucking Inc.* for personal and business use, granted by management of the company. This may be restricted or altogether removed at any time, and employees bear the responsibility to appropriately make use of this benefit. In order to ascertain that all employees of *Planet Express Trucking Inc.* are able to utilize this privilege to its full extent without putting the company at any risk, we have restricted the list of suitable devices to the following:

Here we define what BYOD is, why we need it, and what it means to use it appropriately. Be sure to ascertain the company retains full control and zero liability for any issues. Cover more cases for > 1 pages

- iPhone 5s through iPhone 7 and 7 Plus (including iPhone SE)
- Samsung Galaxy S6 and S6 Edge
- Samsung Galaxy S7 and S7 Edge
- Google Pixel and Pixel XL
- LG G5
- Other devices on a case-by-case basis as determined by the IT department
- (The Galaxy Note series has been **banned** for both security and hardware concerns)

Here, cover a list of appropriate devices. Keep it short to save space if necessary, but list a reason why few devices are allowed.

The device of the employee must have the following security precautions:

- A password that complies with company password regulation policy
- A GPS locator application in order for the company to be aware of its location at any time
- The ability to be completely and securely wiped by the company at any time and for any reason
- iPhones and Android devices must **NOT** be “jailbroken” or “rooted.”

Create a list of requirements for any device to meet the standards of the policy. Keep basic security measures in mind.

The privilege to bring personal devices for use with work-related activities directly relies on employees to self-monitor their usage in order to assure that the policy is not taken advantage of. What is considered inappropriate use of the policy is at the company’s discretion and the employee agrees to comply with all company regulations policies, both within the workplace and outside of it. It is suggested that employees verify with management that their specific use cases comply with company policy and device management regulations. Any violations will be addressed by the company and employee directly, and appropriate discipline will be administered. This includes but is not limited to:

Cover situations that will result in lost privileges. Be very explicit because legally speaking, people like to think that they can do anything not specifically prohibited. Make sure to mention that we can take it away for *any reason* we want.

- Inappropriate use of device

- Using device for activities that harms the company
- Visiting prohibited websites
- Destruction, corruption, or theft of company property

Release of Liability: Make it legally tight by telling the employees that anything bad they do is on them.

The employee releases *Planet Express Trucking Inc* from all liability associated with data loss, bugs, failures, or other issues related to the company that may occur. The employee is aware of the risks at hand and assumes all responsibility for stolen company data, unauthorized access due to the employee's device, and other negative repercussions associated with the device.
If you have more room, go into deep detail about everything you can define. We're likely to be restricted to one page, so keep it short and sweet, but the more room you have, talk about the reprecussions for both the employee and the company for violating the policy, the risks being taken by the company, and the trust the company is placing in the employee. The above is a truncated example, so adjust to the situation as needed. When in doubt, ban. Write it as though it would be used in court, so make sure it's very clear what can and cannot be done. Follow this structure: Definition and Overview—Devices—Ownership/Payment (if enough space. Optional)—Security Requirements—Acceptable Use—Release of Liability and Other Legal Information.

Password Policy

Password Policy is most likely going to be rather short and probably will be implemented in a Group Policy Object rather than just in words. But if a policy needs to be written, a password policy will be much more objective and less verbose than other policies tend to be. It consists of a set of rules to follow rather than a description of information employees should know.

Open with a description of why password policies are necessary if a longer version is desired.

Complexity:

- Passwords must meet minimum length of **six** characters (increase if necessary).
- Passwords must contain at least **three** of the following: Capital letters, lowercase letters, numbers, or symbols.
- Passwords must not be common words or names. They must not be able to be easily guessed.
- Every **X** days, the password must be changed (alter time as needed)
- New passwords cannot resemble previously used passwords in any way

Responsibilities of Employee:

- The employee will never reveal their password to anyone
- The employee will not communicate their password under any circumstances
- The employee will not store his password in any format or medium, including text message, email, password storing applications, paper, etc.
- Do not use “Forgot Password” options as offered by some web services to recover passwords related to the company.
- In return, the company will not share the password of the employee with anyone, including the employee. If the employee forgets their password, they must contact IT for it to be reset.

If they only ask for rules, just include above. If they want a policy, include the following:

Repercussions for Violating Policy:

- If the company is harmed due to irresponsible actions of the employee, the employee will be immediately suspended and appropriate legal recourse will be taken. Under extreme circumstances, the employee may be terminated.
- If the employee violates password policy but no measurable damage to the company is done, the recourse of the employee will be determined by their supervisor.
- If the employee reports potential issues with their password in accordance to the policy, the violation may be lifted at the discernment of the supervisor.
- If the employee violates password policy in regards to Bring Your Own Device Policy, refer to the BYOD document for information about proper recourse.
- Any employee suspected of password policy violation must issue a report to management to determine the scope of the issue.

  Tweak the above as needed and add anything that might be required by the inject. This may be situation specific, so follow the instructions of the CEO and follow the model.

Telematics Tracking and Retention Policy

1. Overview

Telematics systems provide valuable information to Planet Express Trucking Inc. (hereafter referred to as PETi). Data from this system can be used to more efficiently allocate resources and better serve customers with increased accuracy of delivery times. These systems also serve to protect and support employees of PETi by providing status updates on the safety of PETi vehicles, communications with IT and other support, and more accurate vehicle tracking for emergency and other uses.

Despite the many benefits of telematics, PETi believes it is crucial to openly communicate the process with employees. Because data such as GPS information is collected and tracked, PETi strives to communicate this fully to employees along with the safeguards PETi has put in place to protect employee privacy.

2. Purpose

This policy outlines the data collected by PETi, the restrictions on usage and storage of this data, and the privacy protections and compliance requirements for all employees.

3. Scope

All PETi vehicles include telematics devices to collect data including but not limited to the following:

- Vehicle maintenance status
- Location
- Accidents

All PETi employees are expected to follow the guidelines in this policy for data collection and retention and privacy assurance.

4. Policy

4.1 Appropriate Use of Telematics Data

- All data collected by PETi is intended to provide increased value to customers by efficiently
    - Tracking progress of shipments
    - Monitoring vehicle status and safety to protect drivers and schedule maintenance
    - Provide reliable communication to PETi drivers to quickly solve unexpected problems as they arise
- PETi will annually review information needs with the goal of limiting unnecessary data collection.

4.2 Required Use

- Any vehicle owned by PETi must use the telematics system.
- Vehicles operated by but not owned by PETi must either use the telematics system or receive special approval to operate without the telematics system from the PETi Legal team.

- Employees are not liable for telematics service disruptions due to routine or unavoidable equipment malfunction or for other situations deemed outside their control (e.g. break in).
- In the event of a routine or unavoidable equipment malfunction, employees must contact PETi technical support (contact information stored in all company vehicles) to notify them of the problem as soon as able. PETi understands this notification may not always be immediate due to degraded communications from telematics disruptions.
- Employees must not tamper with, damage, or in any way impair PETi's ability to operate the telematics system at full capacity. Employees are liable for any actions they take to affect PETi telematics (directly or indirectly).
- Employees are liable for actions taken by any passengers they be transporting unless the passengers are customers or employees of PETi in which case the passengers are deemed "outside the employee's control".

4.3 Disclosure Restrictions

- Data collected by PETi telematics systems will solely be used for company processes and process improvement.
- Data will not be disclosed or shared with third parties except as required by law in order to protect the privacy of PETi, their employees, and their customers.

5. Policy Compliance

5.1 Enforcement

Potential violations of this policy will be monitored through PETi IT and Operations teams' routine monitoring and usage of the telematics system and routine audits. Investigations regarding potential improper usage or actions of employees regarding telematics will be completed by PETi IT.

Allegations of misconduct of employees' data handling or usage of telematics systems will be referred to PETi HR and Legal. Violation of the terms in this policy may result in disciplinary actions including but not limited to verbal or written warnings, temporary suspension of PETi vehicle operation privileges, or termination.

5.2 Changes and Challenges to this Policy

- Any changes to this policy must be approved by PETi IT, Legal, and the CEO.
- Employees will be notified of any changes to this policy.
- Employees retain the legal right to challenge this policy or future changes with PETi Legal or their own private representation at any time.

PCI Compliance Memo

Currently PETi is **not PCI-DSS compliant**. If PETi does not become compliant, **the company could be liable** for all costs from potential security breaches.

1. If all services continue to be maintained internally, PETi could become PCI-DSS compliant within **three business days** with the cost of considerable manpower from both IT and Legal. However, PETi would have to go through code reviews and get a **PCI PA-DSS certification** on our ecommerce website requiring an **indefinite period of additional internal and external audits**.
2. If the payment portal is outsourced to a company such as Stripe for payment processing, PETi could meet all technical requirements (not including employee training) within **one business day**. While creating an **additional cost, this mitigates liability** in PETi's current services for data breaches and associated legal costs.

Please see the matrix below for more detail on where our current security controls need to be expanded for full compliance.

Goals	PCI DSS Requirements	Requirement Met
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data	**Yes**, using network wide firewall + local firewalls on each system. Internally audited regularly.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	**Yes**, all accounts have been audited to follow the company password policy.
Protect cardholder data	3. Protect stored cardholder data	**No**, cardholder data storage must be secured, removed, or outsourced depending on business needs.
	4. Encrypt transmission of cardholder data across open, public networks	**In Progress**, encrypted transmission is currently being added to website(s) and portals.
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs	**Yes**, antivirus is installed and monitored on all systems.
	6. Develop and maintain secure systems and applications	**Yes**, services are patched and monitored.
Implement strong access control measures	7. Restrict access to cardholder data by business need to know	**Yes**, cardholder data access is restricted and any attempts to access/change this data is monitored in real time.
	8. Assign a unique ID to each person with computer access	**Yes**, but if employees need remote network access in the future, additional controls will be required.
	9. Restrict physical access to cardholder data	**Yes**, the IT manager is responsible for enforcing physical security policies.

Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data	**Yes**, all logs and audit trails are remotely stored and backed up offline regularly[AR1] .
	11. Regularly test security systems and processes	**In Progress**, an external testing vendor must be contracted for full compliance.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel	**In Progress**, some policies have been created by IT, but further training and planning is needed.