# An Intergalactic Delivery Company

“Our crew is replaceable. Your package isn’t!”

# Table of Contents

# Policies

## Introduction

The following policies shall be followed by any and all Planet Express employees. Failure to do so will result in a written report to the manager who oversees the person who infringes the policy. Disciplinary action will be taken.

These policies are not suggestions, but rather “set in stone” rules that must be followed in order to ensure the success, safety, and trust of Planet Express.

## Ethics Policy

### Introduction

Planet Express strives to create and maintain a culture of trust and integrity throughout all aspects of the business. Strong ethics is a team effort put together by every member of the planet express team. All employees should familiarize themselves with the contents of this policy in order to maintain a strong and robust ethics culture. Planet Express is committed to protecting both our customers and our employees from malicious and/or illegal activities from individuals who were aware or unaware of their actions. Planet express holds every single employee to the highest level of accountability when it comes to ethics and any breach in these policies will not be tolerated and may lead to termination.

### Purpose

The purpose of writing this policy is to highlight the expectation of both the employees and customers to be treated fairly within Planet Express. This document will serve as guidance for all employees to ensure ethical behavior.

### Scope

This policy applies to all employees, sub-contractors, seasonal employees, and others employed at Planet Express.

**Policy**

1. **Leadership**

Employees in leadership positions must set a prime example for their teams to follow. Honesty and integrity are your top priority. LEaders must have an open-door policy for any and all employees on their team as well as welcome any suggestions from the team. Leaders must disclose any potential conflicts of interest they may have.

2. **General Employees**

Planet Express and its employees will treat everyone with respect and promote an inclusive team environment. Every employee must to the best of their ability to demonstrate ethical behaviors and business practices. Employees must disclose any potential conflict of interest they may have.

3. **Company**

Planet Express will promote ethical behavior with incentives for ethics that are observed. Planet Express will promote trustworthy and honest interpersonal communications within the company to reinforce our vision for strong ethics within the company.

4. **Unethical Behavior**

   Planet Express will avoid the intent of unethical business practices, relationships, and communications. Planet Express will not tolerate discrimination based on but not limited to, creed, sexuality, race, planetary origin, number of legs, eyes, tentacles and other extremities. Planet Express will not tolerate any unauthorized use of proprietary or confidential company information. Employees will not use company assets for personal gains.

5. **Enforcement**

Any infractions of this ethics code will not be tolerated. Any and all employees found acting unethically will be subject to disciplinary action up to and including termination.

## Internet Use Policy

The following guidelines are designed to help you make the most out of Internet resources. You should understand all of the following:

1. Planet Express provides internet access to our staff in order to assist them in carrying out their duties. It is assumed that the internet will be used to look up details about suppliers, products, to access government information, and other statutory information.
2. You may only access the internet by using Planet Express's software, firewall, and router.
3. You may only access the internet after your department manager has authorized you to do so in writing.

When using Planet Express's internet access facilities, you shall comply with the following guidelines:

DO:

4. Keep your use of the internet to a minimum.
5. Check that the information you access is accurate, complete, current, and safe.
6. Respect the legal protections of data and software provided by copyright and licenses.
7. Inform our IT department immediately of any unusual occurrence.

DON'T:

8. Download text or images which contain pornographic content, racist or extreme political nature, or which incites violence, hatred, or any illegal activity.
9. Download content from internet sites unless it is work related.
10. Use Planet Express's computers to make unauthorized entry into another computer or network.

11. Disrupt or interfere with other computers or network users, services, or equipment. This is a crime under the Computer Misuse Act of 1990.
12. Represent yourself as another person.
13. Use internet access to transmit confidential, political, obscene, threatening, or harassing materials.

<u>PLEASE BE AWARE:</u>

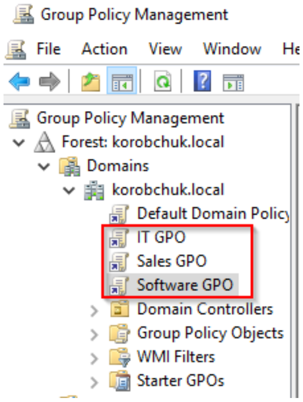
- All of your activity on the internet is monitored and logged.
- All material will be scanned for viruses.
- All of the content viewed is scanned for offensive material.

If you have any doubt about an issue with internet access, consult our IT department.

Any breach of this policy will lead to disciplinary action.

## Group Policy

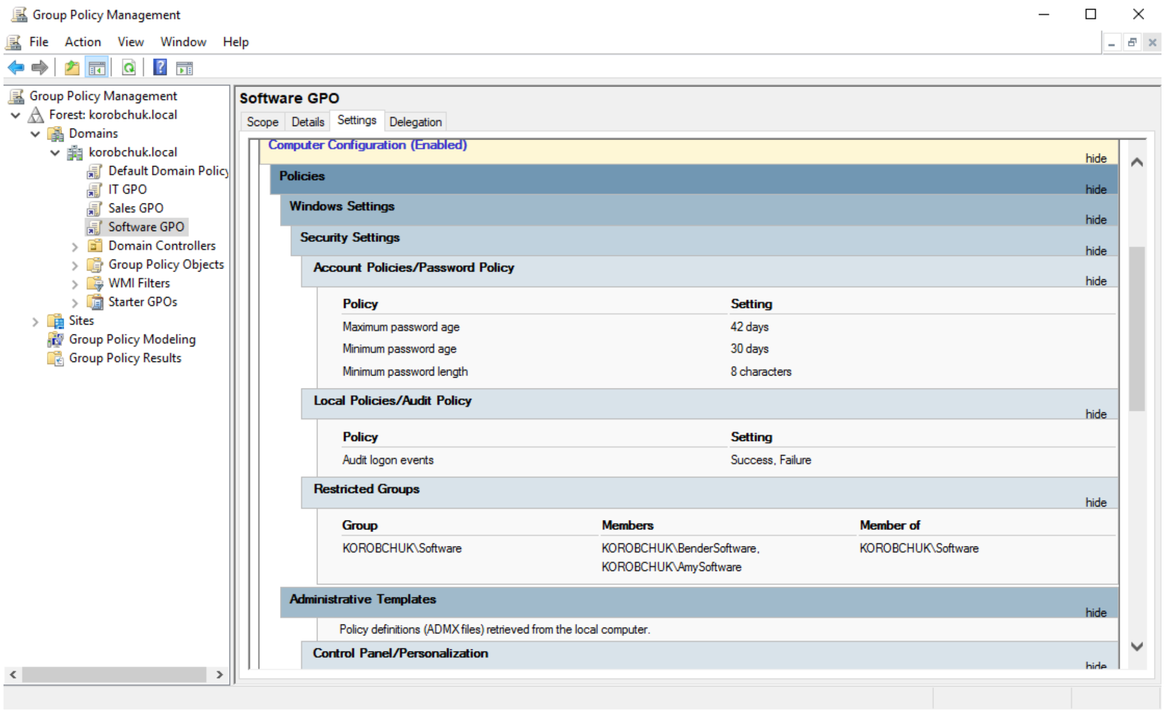
The following are screenshots of our Group Policy.



Group Policy Management
Forest: korobchuk.local
Domains
korobchuk.local
Default Domain Policy
IT GPO
Sales GPO
Software GPO
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs

*Showing three group policies, for the three different groups of our company*

*The following screenshots are displaying the Software GPO*



**Software GPO**

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

| Policy | Setting |
|---|---|
| Maximum password age | 42 days |
| Minimum password age | 30 days |
| Minimum password length | 8 characters |

Local Policies/Audit Policy

| Policy | Setting |
|---|---|
| Audit logon events | Success, Failure |

Restricted Groups

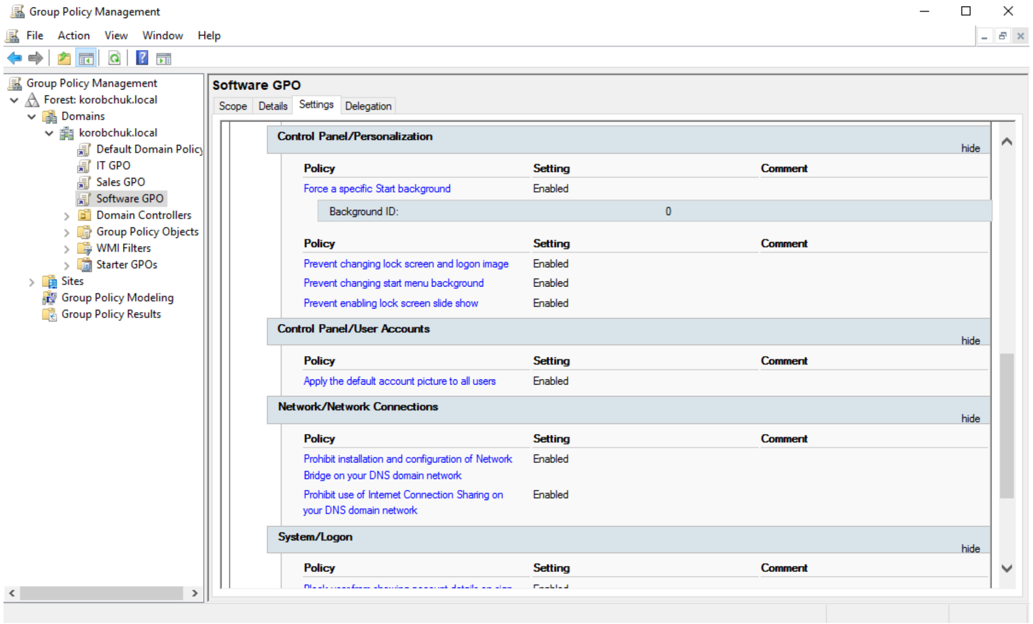
| Group | Members | Member of |
|---|---|---|
| KOROBCHUK\Software | KOROBCHUK\BenderSoftware,<br>KOROBCHUK\AmySoftware | KOROBCHUK\Software |

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel/Personalization

*Showing the password policies, as well as auditing the logon events; including successful and failed attempts*



**Software GPO**

Control Panel/Personalization

| Policy | Setting | Comment |
|---|---|---|
| Force a specific Start background | Enabled | |

Background ID: 0

| Policy | Setting | Comment |
|---|---|---|
| Prevent changing lock screen and logon image | Enabled | |
| Prevent changing start menu background | Enabled | |
| Prevent enabling lock screen slide show | Enabled | |

Control Panel/User Accounts

| Policy | Setting | Comment |
|---|---|---|
| Apply the default account picture to all users | Enabled | |

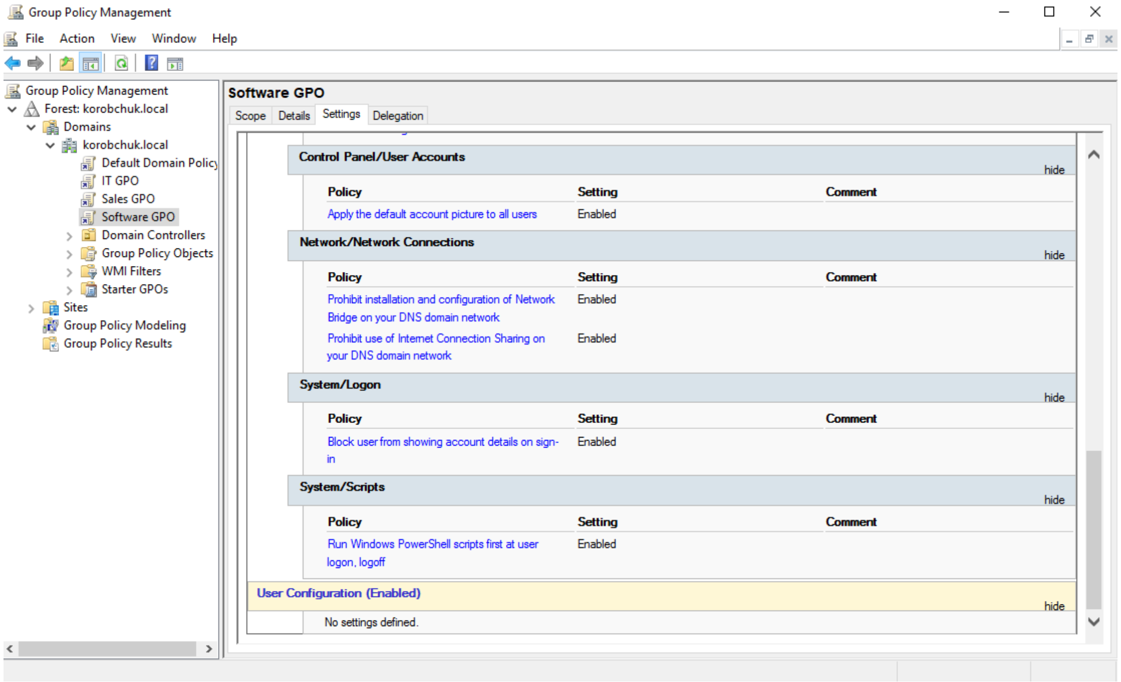
Network/Network Connections

| Policy | Setting | Comment |
|---|---|---|
| Prohibit installation and configuration of Network Bridge on your DNS domain network | Enabled | |
| Prohibit use of Internet Connection Sharing on your DNS domain network | Enabled | |

System/Logon

| Policy | Setting | Comment |
|---|---|---|

*Showing various personalization policies. No changing the lock screen and background images. Prohibit any configuration and installation on the network*



Control Panel/User Accounts

| Policy | Setting | Comment |
|---|---|---|
| Apply the default account picture to all users | Enabled | |

Network/Network Connections

| Policy | Setting | Comment |
|---|---|---|
| Prohibit installation and configuration of Network Bridge on your DNS domain network | Enabled | |
| Prohibit use of Internet Connection Sharing on your DNS domain network | Enabled | |

System/Logon

| Policy | Setting | Comment |
|---|---|---|
| Block user from showing account details on sign-in | Enabled | |

System/Scripts

| Policy | Setting | Comment |
|---|---|---|
| Run Windows PowerShell scripts first at user logon, logoff | Enabled | |

User Configuration (Enabled)

No settings defined.

*Don’t allow the users to show account details on sign in. Run the Windows Powershell scripts at logon*

## Incident Response Policy

Scope
This policy governs the Company's general response, documentation and reporting of incidents affecting computerized and electronic communication information resources, such as theft, intrusion, misuse of data, denial of service, corruption of software, computer- and electronic communication-based HIPAA violations, and incidents reported to Planet Express by its customers and businesses partners. This policy does not include damage to personal computers owned by staff, unless their computers contribute to the Incident defined by the parameters in Definitions, below.

**Policy Statement**

Planet Express and its Security Incident Response Policy and subordinate procedures define standard methods for identifying, tracking and responding to network and computer-based IT Security Incidents.

**Reason for the Policy**

The Planet Express IT Security Incident Response Policy is established to protect the integrity, availability and confidentiality of confidential or proprietary information, including ePHI to prevent loss of service and to comply with legal requirements. This policy establishes the coordination of

Planet Expresses response to computerized and electronic communication systems incidents to enable quicker remediation, information gathering and reporting of infrastructure-affecting and HIPAA-Security related events.

**Definitions**

An IT Security Incident ("Incident") is any activity that harms or represents a serious threat to the whole or part of Planet Expresses computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a "virus," "malware" or similar issue that has little impact on the day-to-day business of the company is not considered an Incident under this policy.

HIPAA Policy 5143 –Planet Express Incident Response Policy

Please also refer to the Master Glossary of HIPAA Security Terms in the Definitions section within Policy 5100 Electronic Protected Health Information Security Compliance.

Policy Sections

5143.1 Identification of Incidents Any employee or customer of Planet Express may refer an activity or concern to the Information Security Office. The ISO itself can also identify an Incident through its proactive monitoring of Planet Expresses network and information system activities. Once identified, the ISO will use standard internal procedures to log and track Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in the remainder of this policy.

5143.2 Establishment of an IT Security Incident Response Team The Information Security Office (ISO) is responsible for Incident interdiction and remediation of computer and electronic communication -based resources affected by these incidents. ISO will consult key representatives of Planet Express ITS, employees in effected offices, Disaster Recovery, and the Legal, Public Affairs, Internal Audit, Administrative Systems Departments, or other units, as warranted, to establish an IT Security Incident Response Team appropriate to respond to a specific Incident. .

5143.3 Risk Assessment Classification Matrix The ISO will establish an internal risk assessment classification matrix to focus the response to each Incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an "escalation" of contacts across the company and its affiliates, and will indicate which authorities at Planet Express to involve and which procedure would be applicable for each class of incident.

5143.4 Documentation and Communication of Incidents The Information Security Office will ensure that Incidents are appropriately logged and archived. Any IT Security Incidents involving ePHI will be so identified in order to implement the relevant HIPAA Security procedures. Incident reporting will be provided by the Information Security Office Wherever possible, documentation of such Incidents will cross-reference other event databases within the University, such as the Information Security Office trouble ticketing and network monitoring systems. Any Incidents involving systems that are tracked in the Above-Threshold ePHI System Inventory Database will be cross referenced in that database with the ISO incident tracking log.

The Information Security Office or IT Security Incident Response Team representatives will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.
5143.5 Subordinate Procedures The ISO will maintain standard subordinate procedures for the response and investigation of each Incident, as well as securing the custody of any evidence obtained in the investigation. The application of these procedures will be governed by the classification matrix described in Section 0000.3 above. The procedures will specify the location and method of custody for each incident, if custody of evidence is required.
04/20/2005 Page 2 of 4
HIPAA Policy 5143 –Planet Express Incident Response Policy
5143.6 Role of Planet Express, Training Planet Express personnel are required to report Incidents to the Information Security Office. The HIPAA Security training that is required for Planet Express, staff, their supervisors, and managers will cover specific procedures for reporting Incidents involving ePHI.
5143.7 Relationship to State and Federal Agencies A response plan or remediation defined by this policy may be preempted as required or at the discretion of Planet Express by the intervention of federal and state executive officials.
5143.8 Incident Prevention Wherever possible, Planet Express will undertake measures to prevent Incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its IT resources.
5143.9 Modifications and Adjustments This policy and its procedures will be reviewed at least annually to adjust processes, identify new risks and remediations.

**Special Situations/Exceptions**

Any personally-owned devices, such as PDAs, phones, wireless devices or other electronic transmitters which have been used to store ePHI and are determined to contribute to an Incident, may be subject to seizure and retention byPlanet Express until the Incident has been remediated, unless the custody of these devices is required as evidence for a court case. By using these devices within the Planet Express network for business purposes, individuals are subject to Planet Express policies restricting their use.

## Server Backup Policy

**Overview:** This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

**Purpose:** This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

**Scope:** This policy applies to all equipment and data owned and operated by the organization.

**Definitions:**

1. Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

2. Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

3. Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

**Timing:** Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

**Tape Storage:** There shall be a separate or set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate or set of tapes for each Friday of the month such as Friday1, Friday2, etc. Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.

**Monthly Backups:** Every month a monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets.

**Age of tapes:** The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes.

**Responsibility:** The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

**Testing:** The ability to restore data from backups shall be tested at least once per month.

**Data Backed Up:** Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server

3. Production web server
4. Production database server
5. Domain controllers
6. Test database server
7. Test web server

**Archives Archives:** are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

**Restoration Users:** that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

**Tape Storage Locations:** Offline tapes used for nightly backup shall be stored in an adjacent building in a fireproof safe. Monthly tapes shall be stored across the galaxy in our other facility in a fireproof safe.

This policy may contain descriptions about how various systems and types of systems are backed up such as Windows or LINUX systems.

# User Accounts

**IT**

- **Alex**
    - **Account**: SysAdmin
    - **Department**: IT
    - **Group**: IT, Admin
    - Runs and maintains the IT department. Ensures all system patches are installed promptly to maintain system security, as well as keeping all programs up to date.

- **Harrison**
    - **Account:** ITConn, SoftwareConn, SalesConn
    - **Department:** IT
    - **Group:** IT

  - Responsible for connecting workstations. This person has three accounts for each department for auditing purposes.
- **Chris**
  - **Account:** ITBack
  - **Department:** IT
  - **Group:** IT
  - Responsible for backing up the server every weekend.
- **Fry**
  - **Account:** ITLogger
  - **Department:** IT
  - **Group:** IT
  - Observes all system logs for Planet Express.
- **Professor Farnsworth**
  - **Account:** SalesACC, SoftwareACC
  - **Department:** Sales, Software
  - **Group:** ITACC
  - Responsible for creating accounts for each individual department. Is the operator of both the Sales and Software local administrator accounts.

### Sales

- **Leela**
  - **Account:** LeelaSales
  - **Department:** Sales
  - **Group:** Sales
  - Keeps track of the different options and choices for shipping.
- **Hermes**
  - **Account:** HermesSales
  - **Department:** Sales
  - **Group:** Sales
  - Takes and uploads the photos of the work environment and boxes so potential customers can see how clean and tidy Planet Express is.

## Software

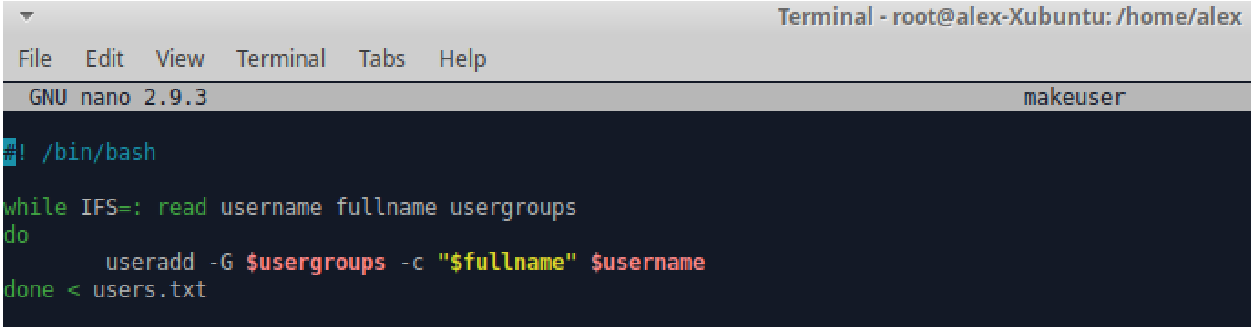
- **Amy**
  - **Account:** AmySoftware
  - **Department:** Software
  - **Group:** Software
  - Responsible for keeping the website up to date and making the website look nice.
- **Bender**
  - **Account:** BenderSoftware
  - **Department:** Software
  - **Group:** Software
  - Ensures the money is properly transferred when people make transactions. Totally doesn’t steal any…

## None

- **Dr. Zoidberg**
  - **Account:** Zswizzle
  - **Department:** None
  - **Group:** None
  - No permissions allowed, don’t let him near a computer. He’s only here because he’s Professor Farnworth’s oldest friend. Don’t let his name fool you, he knows nothing about the human body.

# Scripts

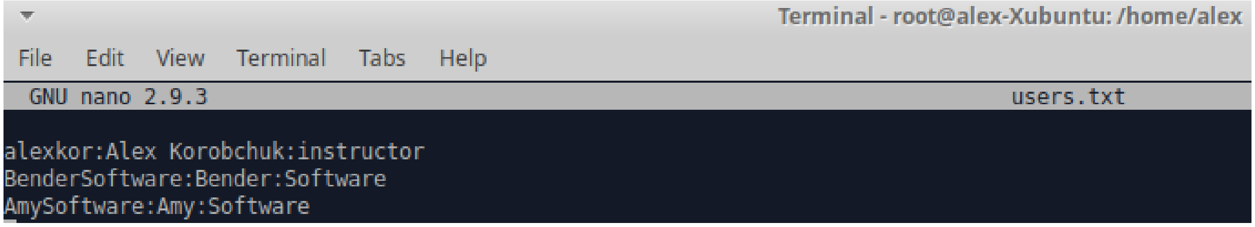
## Linux


Terminal - root@alex-Xubuntu: /home/alex
File Edit View Terminal Tabs Help
GNU nano 2.9.3
makeuser

```
#! /bin/bash

while IFS=: read username fullname usergroups
do
        useradd -G $usergroups -c "$fullname" $username
done < users.txt
```

*This script reads user credentials from a text file called “users.txt” and creates users based on that*

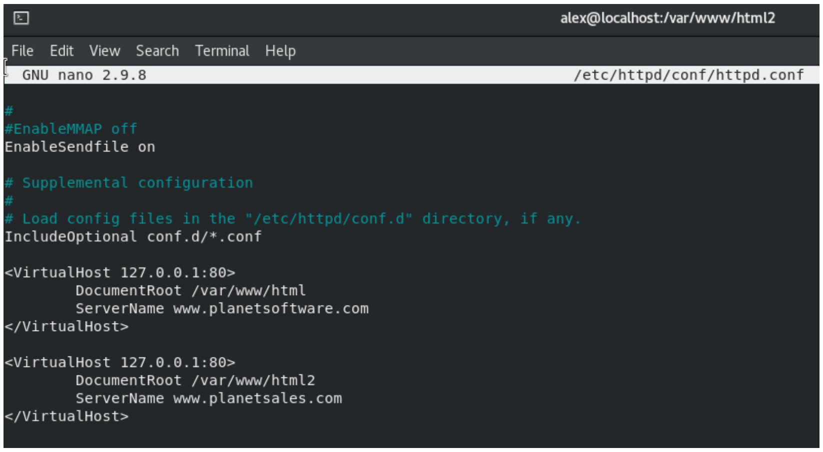

Terminal - root@alex-Xubuntu: /home/alex
File Edit View Terminal Tabs Help
GNU nano 2.9.3
users.txt

```
alexkor:Alex Korobchuk:instructor
BenderSoftware:Bender:Software
AmySoftware:Amy:Software
```

*Example of the users.txt file*

# Websites

Both of the websites are running internally on the network. They are not accessible from the outside world. They are on the CentOS machine.


alex@localhost:/var/www/html2
File Edit View Search Terminal Help
GNU nano 2.9.8
/etc/httpd/conf/httpd.conf

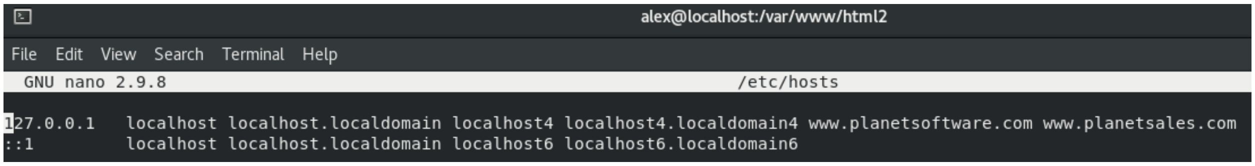
```
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf

<VirtualHost 127.0.0.1:80>
        DocumentRoot /var/www/html
        ServerName www.planetsoftware.com
</VirtualHost>

<VirtualHost 127.0.0.1:80>
        DocumentRoot /var/www/html2
        ServerName www.planetsales.com
</VirtualHost>
```

*Showing the httpd.conf file, where the planet sales and planet software have been configured*

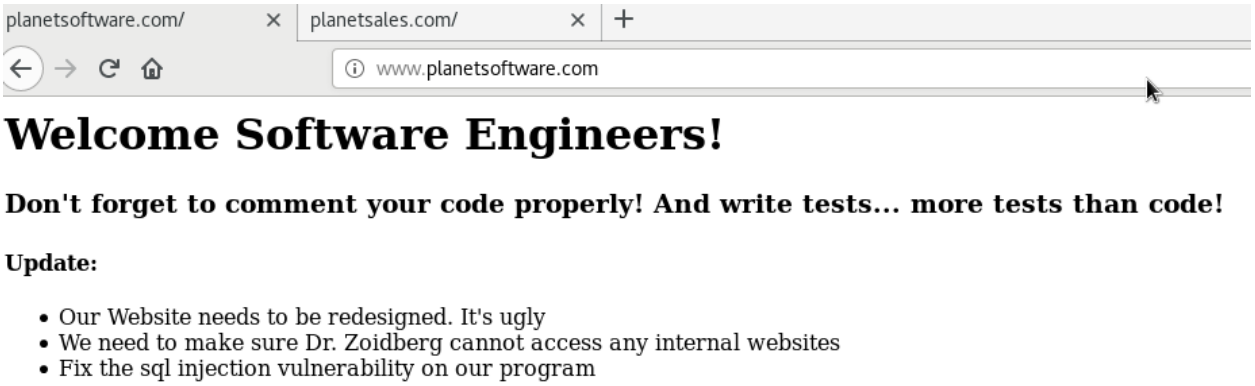

alex@localhost:/var/www/html2
File Edit View Search Terminal Help

```
  GNU nano 2.9.8                                                    /etc/hosts

127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4 www.planetsoftware.com www.planetsales.com
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
```

*Showing the names for the websites*

### Software



# Welcome Software Engineers!

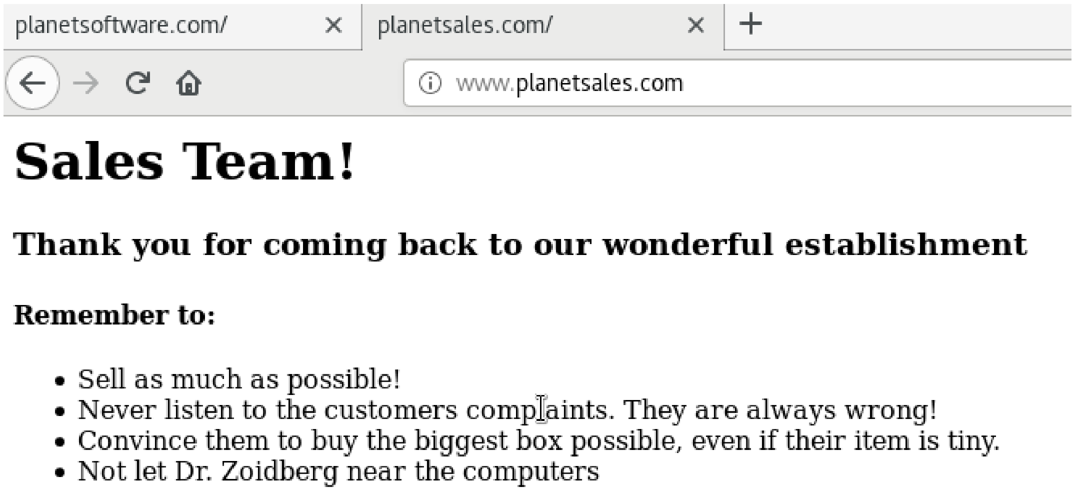
### Don't forget to comment your code properly! And write tests... more tests than code!

**Update:**

- Our Website needs to be redesigned. It's ugly
- We need to make sure Dr. Zoidberg cannot access any internal websites
- Fix the sql injection vulnerability on our program

*Showing the website for the software team*

### Sales



# Sales Team!

### Thank you for coming back to our wonderful establishment

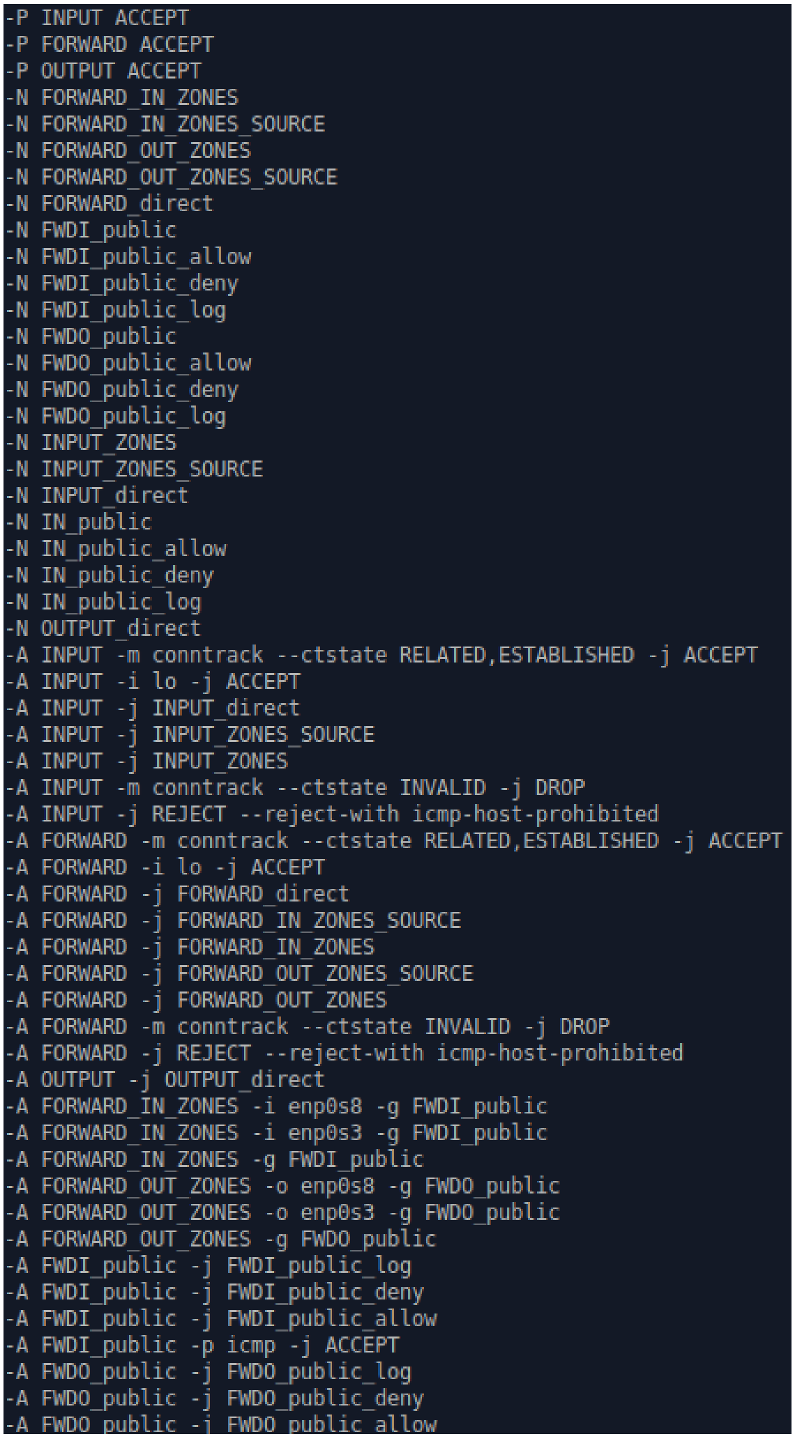
**Remember to:**

- Sell as much as possible!
- Never listen to the customers complaints. They are always wrong!
- Convince them to buy the biggest box possible, even if their item is tiny.
- Not let Dr. Zoidberg near the computers

*Showing the website for the sales team*

# Linux Documentation

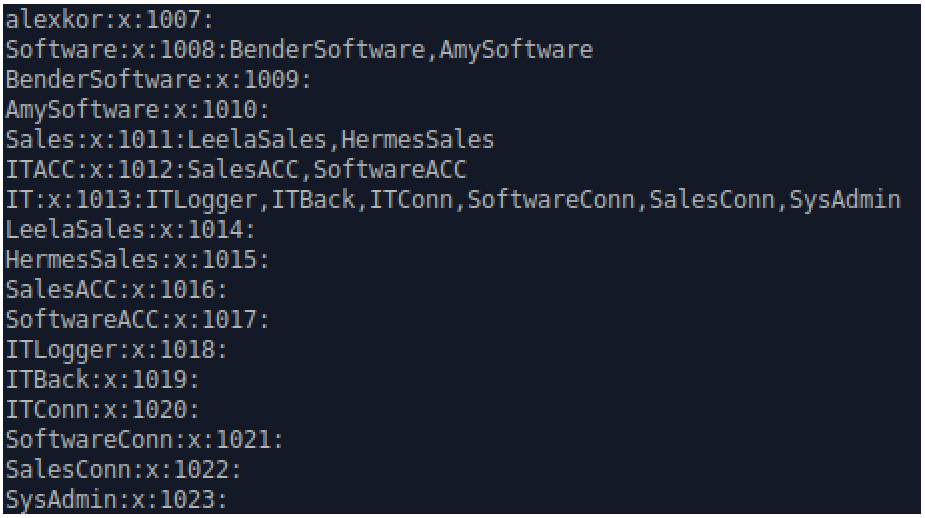
## Firewall rules



```
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-N FORWARD_IN_ZONES
-N FORWARD_IN_ZONES_SOURCE
-N FORWARD_OUT_ZONES
-N FORWARD_OUT_ZONES_SOURCE
-N FORWARD_direct
-N FWDI_public
-N FWDI_public_allow
-N FWDI_public_deny
-N FWDI_public_log
-N FWDO_public
-N FWDO_public_allow
-N FWDO_public_deny
-N FWDO_public_log
-N INPUT_ZONES
-N INPUT_ZONES_SOURCE
-N INPUT_direct
-N IN_public
-N IN_public_allow
-N IN_public_deny
-N IN_public_log
-N OUTPUT_direct
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -j INPUT_direct
-A INPUT -j INPUT_ZONES_SOURCE
-A INPUT -j INPUT_ZONES
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i lo -j ACCEPT
-A FORWARD -j FORWARD_direct
-A FORWARD -j FORWARD_IN_ZONES_SOURCE
-A FORWARD -j FORWARD_IN_ZONES
-A FORWARD -j FORWARD_OUT_ZONES_SOURCE
-A FORWARD -j FORWARD_OUT_ZONES
-A FORWARD -m conntrack --ctstate INVALID -j DROP
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -j OUTPUT_direct
-A FORWARD_IN_ZONES -i enp0s8 -g FWDI_public
-A FORWARD_IN_ZONES -i enp0s3 -g FWDI_public
-A FORWARD_IN_ZONES -g FWDI_public
-A FORWARD_OUT_ZONES -o enp0s8 -g FWDO_public
-A FORWARD_OUT_ZONES -o enp0s3 -g FWDO_public
-A FORWARD_OUT_ZONES -g FWDO_public
-A FWDI_public -j FWDI_public_log
-A FWDI_public -j FWDI_public_deny
-A FWDI_public -j FWDI_public_allow
-A FWDI_public -p icmp -j ACCEPT
-A FWDO_public -j FWDO_public_log
-A FWDO_public -j FWDO_public_deny
-A FWDO_public -j FWDO_public_allow
```

*All of the firewall rules*

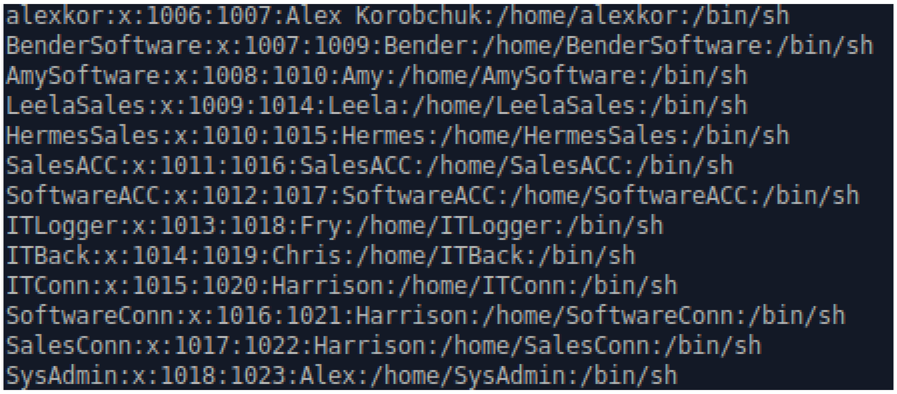
## Groups



```
alexkor:x:1007:
Software:x:1008:BenderSoftware,AmySoftware
BenderSoftware:x:1009:
AmySoftware:x:1010:
Sales:x:1011:LeelaSales,HermesSales
ITACC:x:1012:SalesACC,SoftwareACC
IT:x:1013:ITLogger,ITBack,ITConn,SoftwareConn,SalesConn,SysAdmin
LeelaSales:x:1014:
HermesSales:x:1015:
SalesACC:x:1016:
SoftwareACC:x:1017:
ITLogger:x:1018:
ITBack:x:1019:
ITConn:x:1020:
SoftwareConn:x:1021:
SalesConn:x:1022:
SysAdmin:x:1023:
```

*Output of the /etc/groups file*

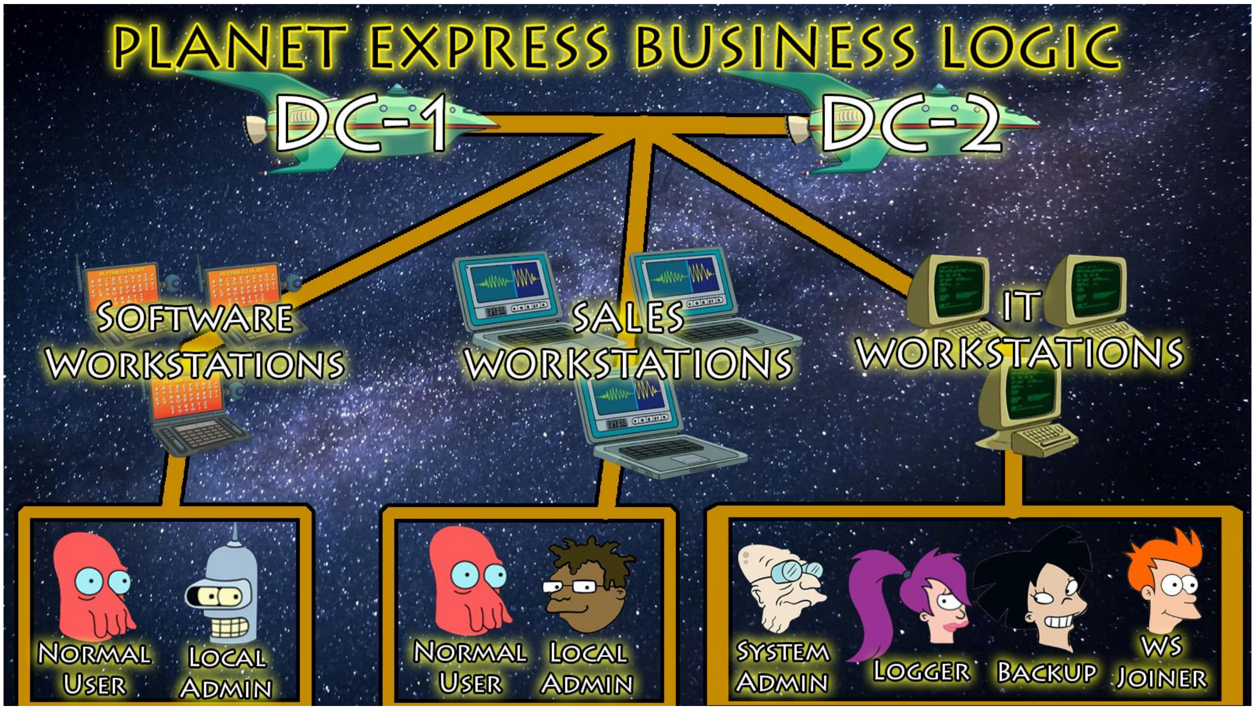
## Passwd



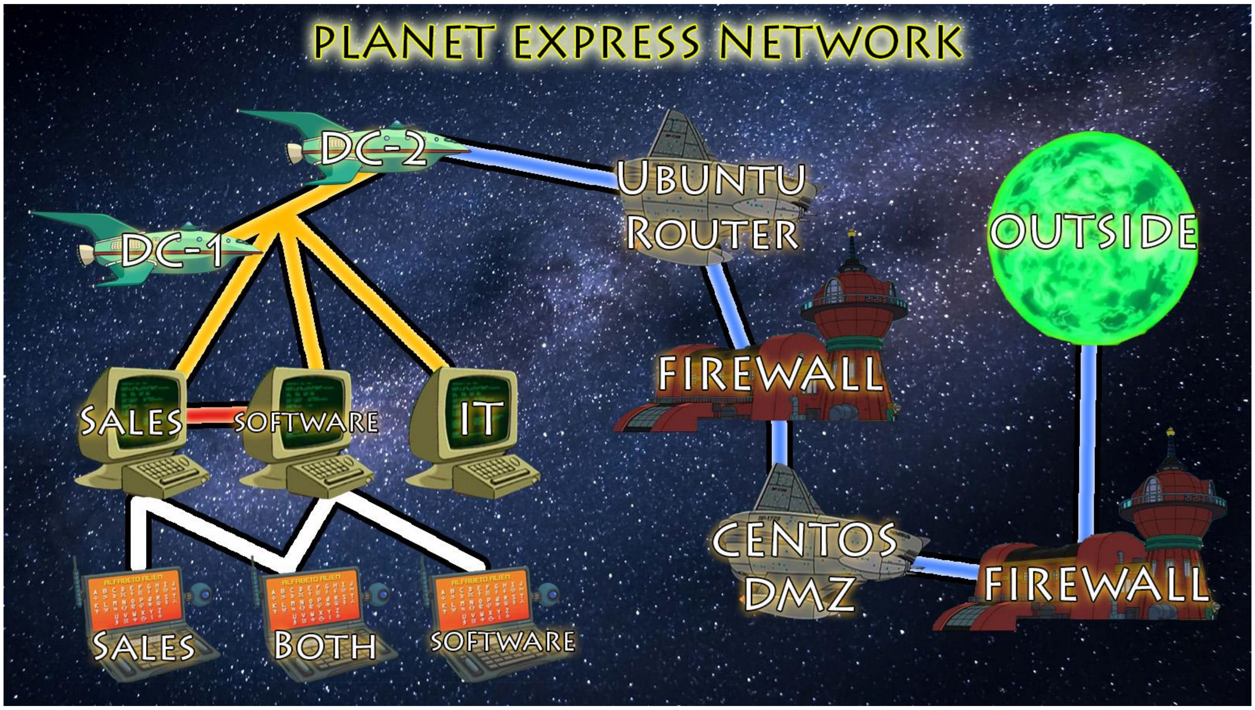
```
alexkor:x:1006:1007:Alex Korobchuk:/home/alexkor:/bin/sh
BenderSoftware:x:1007:1009:Bender:/home/BenderSoftware:/bin/sh
AmySoftware:x:1008:1010:Amy:/home/AmySoftware:/bin/sh
LeelaSales:x:1009:1014:Leela:/home/LeelaSales:/bin/sh
HermesSales:x:1010:1015:Hermes:/home/HermesSales:/bin/sh
SalesACC:x:1011:1016:SalesACC:/home/SalesACC:/bin/sh
SoftwareACC:x:1012:1017:SoftwareACC:/home/SoftwareACC:/bin/sh
ITLogger:x:1013:1018:Fry:/home/ITLogger:/bin/sh
ITBack:x:1014:1019:Chris:/home/ITBack:/bin/sh
ITConn:x:1015:1020:Harrison:/home/ITConn:/bin/sh
SoftwareConn:x:1016:1021:Harrison:/home/SoftwareConn:/bin/sh
SalesConn:x:1017:1022:Harrison:/home/SalesConn:/bin/sh
SysAdmin:x:1018:1023:Alex:/home/SysAdmin:/bin/sh
```

*Output of the /etc/passwd file*

# Network/Business Logic Diagrams



*The Planet Express business logic diagram*



*The Planet Express network diagram*