Sports 4 U Report

# Sports 4 U Network Requirements:

* **Internet Connection (ISP)**

This is needed to connect to the internet so the organisation can access the system over the Web and so the company can setup a website for their business.

* **Router**

A router is needed to connect the network we’ll be setting up for them to the internet. This device is used for traffic routing over the Web.

* **Switch**

The switch is needed because it allows us to connect multiple computers, servers and devices to the network.

* **Web Server**

The company wants to setup a website for their business so a web server is needed to host the website when it is created. It’s also needed to make the created website visible to the rest of the internet.

* **SFTP (Secure FTP File Transfer Server)**

The company wants a secure way of accessing files over the internet from a central location; as such a SFTP Server is required as it allows you to access files on a network from any other device that is connected to it. An SFTP Server uses SSH to encrypt all packet communication so will also be sufficiently secure.

* **Print Server**

Sports4u are going to have a lot of printers on the premises and may sometimes require a way in which to print content onto another printer in another area of the company.

* **Mail Server**

Sports4u have requested they have an internal mail server for use in sending and receiving E-Mails.

* **Multiple User Accounts**

There will be multiple people using the server and thus multiple user accounts are needed.

* **Multiple User Access Levels**

For security purposes, different access level for the user accounts will be needed to be setup.

* **Wireless Access Point**

This will provide wireless access for the Field Sales Staff to the network.

* **Ethernet (CAT6)**

This will be the cabling that is used to connect all of the individual components of the network together.

Interconnection Devices

# Routers:

A router is device used in networking that takes care of routing traffic from computers and others devices over a network. You will find routers in any network that has interconnecting devices because the router is the device that moves the data (commonly in the form of packets) around a network. Routers work with a table type system upon which it has a bunch of IP information. All the devices on the network will have an IP; the router will have this IP in its database as-well as information about the route it has to take to get data to that IP. When you send data from one P.C to another it will check if it knows the destination route, if It does it will route the data to its destination, however if it doesn’t then it will send the data to another router and ask if it knows the route to the destination. It does this until the data gets to its destination or until it times out (if there is no connection). Routers tend to have several ports for connection on them; these will consist of both Ethernet and possibly Fibre or COAX connections.

# Switch:

A switch is a device that works in a similar way to a router and allows you to connect multiple devices together to make a network such as a LAN. The main difference of the switch is it doesn’t start off knowing where to send the data so at first when you have multiple devices connected to it and you want to send data out over your network to a specific device, it will first broadcast said information out over the whole network and the receiving computer will then accept it, it’s at this point that the switch logs the route in which the data has taken to get to that destination. In essence the switch does not know where to send data at first however it learns and logs the routes into a database that it then saves for future reference. It’s also worth noting that much like the router, a switch will delete all its database logs every so often at which point the data will have to be rebroadcasted over a network so it can learn the routes again. A switch is normally a lot faster than a router and tends to have speeds of upwards of 1Gbit/s, they also have several ports that are normally all Ethernet ports unless you need one with Fibre connections, these devices have anything from 5 to 50 Ethernet ports.

# Wireless Access Points

A wireless access point works exactly like you might think, it allows you to put a point of access for your wireless network somewhere in your home or building. You can use wireless access points in several ways: the first is you can position the access points so that you are in essence boosting your signal distance, you do this by placing the access point where it is in distance of your standard wireless hub however far enough away to extend the overall coverage. The second way you could use an access point is to gain wireless coverage in an area where you may not have coverage from a standard wireless hub and where range extension would be ineffective. To do this you may have a wired connection into the area where you are placing your range extender which would allow you to have wireless coverage in that area too. You could also use wireless access points to create wireless hotspots for your network that would allow others to take advantage of your network.

Network devices

# Workstations

A workstation is normally any type of computer or computing device that connects to an external server service. A good example of this would be a dummy terminal system such as the one used in The Sheffield City College, in one room in the College the computers operating system is ran from a server, this is known as an NOS or network operating system. These are seen as workstations as they simply allow you to access and use the resources of the server machine on the other side. Workstations tend to be rather useful as they allow you to connect to servers or systems that may be a lot more powerful than a normal computer system.

# Print Servers

A print server is usually a server that handles one or more networked printers and also handles the prints that are sent to them. It has a queuing based system that allows multiple people to print work if they wish and is normally a first come first serve type system. There are exceptions to the first come first serve type system though and that comes in the form of a priority system, for example if a member of staff decided to print some work, they can choose to print their work sooner than the others. Print servers also add another layer of monitoring to the printers in form of an administration system. On most modern print servers you will have an admin system that allows you to control what the printers do and who has access to them, this is a major benefit when you have multiple user classes. Print servers normally use TCP/IP to transfer the file to the printer ready for printing.

# Mail Servers

A mail server is a server that handles the transfer of E-mail messages. When you send an email you aren’t sending it to the other persons computer, you are actually sending it to the mail server at which point the person you are sending it to can request the email from the server. A mail server simply allows you to send messages in mail form over the internet to other people around the world for practically nothing.

# File Servers

A file server is a server that allows users to connect to a centralized system to upload or download files. These systems are useful because they allow you to have a central area to store all your files if you wish. File servers also tend to have more security as you have to access them over a network; this means you have to access them with a username and password. File servers normally use the FTP protocol in port 21 or 22 depending on if you’re using SSL or not. File servers once again offer a massive amount of control through things like the admin panel.

# Web Servers

A web server is a server system that allows you to host web pages on the internet for others to access and view. The main purpose of the webserver is to host web pages that you or others create from a machine that can be accessed over the internet. The general features most web servers will have include the web hosting service itself which is normally something along the lines of apache. It will also have security features built into it in the form of an HTACCESS system that makes it so that you can set access rights for each of the files on your webserver. You also have SSL as part of most web servers these days.

# Proxy Servers

A proxy server is something that allows you to monitor and control all traffic that passes through it. It does this by sitting between the internet and the terminal you’re using. This allows the proxy server to see everything that passes through it and control everything that passes through it too. A proxy server adds a lot of security for a network as it allows you to control the flow of data within your network and block things you don’t want people to access. It also allows you to block all incoming traffic and monitor it as you can simply disallow all incoming connections except the ones you have set to allow.

# NIC (Network Interface Cards)

A NIC is a device that allows your computer, servers or networked media device to connect to the internet via the communication mediums you are using. The most common one used is Ethernet; a NIC would allow you to connect to the rest of your network as it has an Ethernet access port on it. Most NIC’s will use Ethernet however some are designed for other connection mediums such as Fibre Optic. These cards normally plug into your computer system via PCI or PCI-Express and will have a maximum of around 5 ports.

Connectors & Cabling

# Leased Line

A leased line is a type of internet connection that allows you to connect to the World Wide Web and other computers around the world. The most commonly used leased line type would be a normal internet service provider and the way it works is that it’s normally a very large internet connection line (normally Fibre Optic these days) upon which you lease out a section of that line. Put simply you are leasing a small portion of the overall connection for internet access. The benefit of this type of line is normally that it’s cheaper. The downside to this type of line is that it’s not very secure and anyone on the same line as you could theoretically gain access to your network and information.

# Dedicated Line

A dedicated line allows you to connect to the rest of the Web much like the leased line however instead of it being a leased type system where you are only using a small portion of an overall large connection you have a dedicated line all to yourself that you can take full advantage of. The advantages of this type of line is that it’s more secure than the leased line and simply allows for more network traffic as you have a whole line to yourself that no one else can use. The downside to this type of network line is that they’re usually very expensive to implement and run.

# Media Types

## STP

A shielded twisted pair is a way of wiring network cables in such a way so the cable itself is shielded from any outside interference. This is especially good for cabling where you are running it through areas of a building that would have a lot of electrical interference from power cables or even just areas where there is a lot of other network cables running which could also cause a lot of interference. The downsides to this type of cable are that it’s more expensive and is normally harder to run through areas where lots of turns and angles are needed for it to run correctly. This is because the cable shielding adds an element of resistance when trying to run it in areas that are hard to get to or areas that require you two do lots of turns with the cable.

## UTP

An unshielded twisted pair is much like the cabling mentioned above however it has no shielding or very little shielding around the cable. The reason this cable is used a lot is that it’s easier to run and cheaper to buy. You can do much sharper turns with this type of cable due to the lack of resistance on the cable. The downside to this type of cable is that it’s a lot more susceptible to outside interference.

## Fibre Optic

Fibre Optic cables are a much newer cabling medium and allow for much faster transfer speeds than that of Ethernet (STP and UPT). This cable using glass fibre to transfer data and the data is sent in beams of light. This theoretically allows you to transfer data at the speed of light which you can imagine is a lot faster than any other cabling medium. This type of cable is also completely unsusceptible to electromagnetic interference.

## Wireless

Wireless technology comes in many shapes and forms, the most basic would be Radio or RF. A wireless radio signal was one of the first wireless mediums to be used on a wide scale and allowed people to communicate over vast distances in real time. Since then there has been many different mediums of wireless communication such as satellite and Wi-Fi. Wi-Fi is however the most widely used wireless communication technology in use today. Wireless allows you to send data over moderately large distances depending on the technology you’re using. It’s good for communicating data in areas where having a wired connection just isn’t feasible.

## Mobile Technology (3G – 4G)

Mobile technology is a lot newer than most other wireless technologies out there and is simply the way of sending and receiving data over the same network your phone calls go through (your mobile service provider). Since then there has been several new implementations of mobile wireless technology with the newest being 4G. 4G allows you to communicate over amazingly vast distances at speeds of up to 50mbit/s.

Software

# Network Operating System

## MAC Server

MAC server otherwise known as O S X Server is a server operating system that is designed to take advantage of the standard MAC operating system as-well as server specific things too. The operating system itself used to be separate on its own however now the server operating system is combined into the OSX package. This means you can take advantage of all the server applications and programs that OSX Server used to have inside the main OSX operating system. OSX Server used to use open directory however now it all uses active directory much like Windows.

Mac Server Operating system: £15

## Linux Server

Linux server comes in many different flavours known as distributions and is probably one of the most widely used server operating systems out there today. It’s an open source system meaning that all files and settings are stored in a plain text format. It does not natively use any form of directory system like MAC Server and Windows server do which does make it a little harder to configure, that being said it also makes it much more configurable than Windows Server and MAC Server. Linux server systems are the most widely used server systems due to their versatility and the fact that it’s free to use.

Linux Server Operating System: Free

## Windows Server

Windows server is a server system that uses active directory to set out uses and permissions. It allows you to set up multiple servers each with its own function inside of the windows server operating system and administrate them all from an easy to use, user friendly GUI.

Windows Server Operating System: £400

# Virus Checker

Virus checker software comes on many different shapes and flavours and many do the same exact thing. The main purpose of the virus checker software is to check all files on your computer as-well as any files you add to your computer in real time. This helps prevent malicious software and attacks coming in the form of viruses from the software you download and install. A virus checking system will usually have a link to an online database system that will allow it to keep up to date meaning it will always be aware of the latest threats that could affect your computer.

# Firewall

A firewall is a device that sits between your computer and the internet and checks all incoming and outgoing data against a set of rules that are set by the user. It will allow or deny connections based upon the rules you set. The main advantage of a firewall is to block any incoming attacks or communication that is incoming to your network. It also allows you to administrate what communications are sent and received on your network.

# Email Client

An E-Mail client is a piece of software that allows you to connect to an E-Mail server to retrieve and send E-Mail media. The most commonly used ones are those found in the complete Microsoft Office Suite and the now online one you can find from Microsoft/Google/Yahoo and many other manufacturers. This software allows you to easily send E-Mails to any E-Mail server on the internet or even within a LAN (Providing the E-Mail server is on the LAN), it also allows you to either retrieve new E-Mails from an E-Mail server or sync E-Mails from the server to the client. The Term “Sync” is simply the process of having your E-Mail client automatically check and retrieve new E-Mails you receive.

Services in the Network Solution

# Directory Services

## DNS:

DNS or domain name server is the protocol that is in charge of translating your IP into a resolvable domain such as bbc.co.uk. This means that rather than having to type in 192.168.0.1 you would instead type in something like bbc.co.uk.

### Good Points:

**1: Allows you to easily access networks or locations upon a network through use of words rather than having to remember hundreds of IP addresses.** This becomes incredibly useful when you consider the amount of IP address that even a small network may have.  
2: **Allows you to organise areas of a network into specific domains that can each have different access rights.** This is useful for security and management areas as it allows you to set out your network into a hierarchy upon which you can apply access rights to easily and manage each section easily.   
**3: Allows you to setup user access rights to specific domains for security purposes.** This adds a nice level of extra security onto your network and allows you to easily setup areas which certain employees can access and which other cant.

### Bad Points:

There are very little downsides to using a DNS service for a company. As stated it allows you to create a hierarchy of domains and user access levels to better control your overall network. There is very little downside to using a DNS.

The one downside I could mention is the setup and control of the DNS. As it’s not something everyone is aware of being able to do and setup, it requires specialist training to control and sometimes that training can cost a lot of money. While it’s not hard to setup and control for an IT savvy person, it would be very alien to someone who doesn’t quite understand computing and thus may take time for them to understand how to use it.

## Active Directory:

Active directory is the directory system used on all windows server system today. Put simply, active directory is a database of user account and access rights which can be modelled and changed to suit the needs of the system developer for a business or even just a normal everyday user. Active directory allows you to store accounts and password as-well as the above mentioned access rights in a central location improving an organisations overall system security.

### Good Points:

**1: Centralised management.** This is very important as it simply increases the efficiency at which your companies system can be managed. Having everything split out everywhere with no cohesion amongst it makes it incredibly hard to both change and keep track of changes and modification you make. Centralising all the information makes it both easier to keep track of, easier to change and edit, easier to add upgrades and extra security and incredibly easier to expand.  
**2: Expandability.** Active directory is created in a way that allows for a massive amount of expandability within any organisation, you can use it in small companies and it will do the job perfectly fine. You can also use it massive businesses too as active directory can have thousands of users all on the system with ease. This added expandability makes it easier to expand your company in the future without having to change very much at all.   
**3: Cost.** The cost of active directory is related to the overall cost of installing windows server onto your network. Due to its expandability, active directory is a very cost effective implementation as after you have it setup there is very little need to every upgrade to anything else.

### Bad Points:

**1: Complexity.** Active directory is a very complex piece of software and is actually rather slow when it comes to its ability to respond to company needs. This is because today it’s very hard to implement into anything that isn’t windows related or linked into the infrastructure it’s designed upon. Which brings me to my next bad point.  
**2: Infrastructure Dependant.** Active directory is very infrastructure dependant meaning that unless you build your whole setup with active directory in mind as the main directory service, you’re going to have a hard time implementing it.   
**3: Age.** Active directory was designed in the 90’s and now it’s simply just old. Active directory isn’t used by big companies such as fortune 500 companies because it’s amazing and the best thing available, it’s used because there infrastructure and systems where built in the 90’s and are very hard to update because of their complexity (two already bad points that I have mentioned). Put simply active directory is only used because it has to be used by most companies. Companies like google and cloud based companies don’t use it anymore as it’s simply too old and takes a lot of time and effort to interface with anything other than windows.

# Telecommunication Services

## E-Mail:

E-Mail is simply the form of sending normal everyday mail like you would get on paper through the letter box however it is sent digitally as an E-Mail (Electronic Mail) over the internet to its destination. This form of mail is both faster and cheaper than conventional mail and is one of the best ways to send mail anywhere in the world. Normally the way mail works is you would have a mail server somewhere in the world and one in your company. You would send mail from your server to the other server at which point the receiver could request the new mail he/she has received to their machine.

## Remote Access:

Remote access is one of the best ways to access a machine from anywhere in the world via use of the internet. Doing this kind of thing is simple and normally only requires you to either install some software into both your P.C you are trying to connect to and the device (let’s say a mobile phone) you are trying to connect from. Then you simply connect using either the domain name or the IP address of the machine you want to connect to and login. This allows you to use the computer like you where sat at it without actually being anywhere near said machine. This form is access is very useful for when you need to do work from home, fix something or edit something on your machine or if you want to use it to help a friend fix something on his/her machine.

# File Services

All network file services include the following things:

## File Transfer:

File transfer is the system that is in place to transfer files from one location to another via use of different protocol. Sometimes that protocol may be ftp which is the file transfer protocol however in more recent years, more protocols have appeared such as samba. In this situation though it will be FTP. FTP allows you to transfer files over a network and over the internet if you so wish from one location to another. This transfer’s speed is dependent on the speed of the network (upload) and your speed as a client (download), it is also dependent on the speed of your hard disk drive and how large the file is as-well as distance it has to travel to its destination.

## File Sharing:

File sharing is much like file transfer however takes advantage of in built systems in the operating system. File sharing enabled operating systems such as Microsoft windows can take advantage of the Access control lists to define what type of access a user has or even if they are allowed access to a folder. As such you are able to setup shared folders and hard drives on a network that have user access levels to govern them. These user access levels can are set within active directory in most cases on a windows network.

# Application Services

## Web:

Web applications come in all shapes and flavours today with the most common being the online E-Mail services offered by google and Microsoft. These services allow you to use them wherever you are as-long as you have access to the internet and run solely on the web. These are amazingly useful in a lot of cases and pretty much everything you could possibly need can be programmed and created on the web today.

## Proxy:

A proxy service is a form of security service that can be used in several different ways. You can first use a proxy for its intended purpose which is to secure and monitor all incoming and outgoing data (traffic) on a network that is connected to the internet. What this allows you to do is limit what websites and people can view of your overall network and von the opposite side you can block employees from going on sites you deem not allowed. Another usage of it is to hide the outgoing traffic of your network, you can use a proxy to fake where the data is going and thus add a further layer of protection to your overall network.

## Print:

Network print services are amazing as they allow you to take advantage of both the printer itself as-well as your network. Simply put, instead of having a USB connection to the printer you have a network connection to it which pretty much acts like having a normal computer connected to it. The up side to having it like this is that you can have the computer miles away from the printer and still print out documents on said printer as-long as you are connected to its network through something such as the internet. It also allows you to have more than one computer linked to the printer, this is useful when you want to keep costs down as it allows you to have 20+ employees and only have 2 or 3 printers (maybe even just the one).

## File Storage:

Networked file storage is useful for several different reasons. The first and most basic reason is it allows you to store your files and data on a machine that is accessible from pretty much anywhere in the world as-long as you have an internet connection to the network the files storage server is on. It also allows you to use it for backup purposes, having a backup is a must have on any system today and especially in a business. By taking advantage of networked file storage you can also make sure that backup is secure and safe away from your company safe from fires, earthquakes, floods etc. Networked file storage simply allows you to store you files on a server somewhere in the world and have it accessible from anywhere that has an internet connection.

## VOIP:

VOIP or Voice over Internet Protocol is a form of communication in which you can talk to someone using a network for free. A VOIP service simply acts like a normal telephone service however the data that is the sound of your voice is converted into digital packets and is sent out over the network to the receiver where it is then converted back into sound that the receiver can listen to and respond.

## Mobile Working:

Mobile working is something that is only available to people because of networks. It is the ability to work away from the computer you normally work at via use of network communication. There are several ways to do this and several ways you can use it too.

### VPN:

VPN or virtual private network is a secure communications network between your computer you wish to connect to and the client device which could be your home computer, laptop, table or mobile phone. A VPN is basically a secure network within the internet in which you use to connect to the computer you wish to work on.

### Remote Desktop (Windows):

Remote desktop is a windows feature that allows you to connect to a computer from anywehere in the world without the need for a VPN. In most cases it’s as simple as clicking a button to activate it on the computer your wish to connect into and then logging into said computer using the IP address of the computer and your standard user login privileges.

### Third Party Applications such as GoToMyPC & TeamViewer:

These are a little bit of a combination of both VPN and Remote desktop, in most cases these application simply allow you to tunnel into your machine via use of a login and they take care of everything like the IP address and other security for you. In most cases these applications are a lot safer than that of the one mentioned above however they’re not all without their downsides.

### Sniffing:

Networking sniffing is where you sit between the computer that is sending the data and the computer that is receiving the data and collect a copy of everything as it passes. You then use complex methods to decrypt and look at everything that both the client machine and the host machine are doing. This is a big problem with mobile working as in essence you are sometimes sending very important information over the most open and most used network in the world, the World Wide Web. As such you need to ensure whichever method you choose to use, you have adequate security in place such as very secure passwords for when you use this type of service.

Security

Every company needs to take one big thing into consideration when they are implanting a network or new service, that thing is security. In most companies there will be a massive amount of very important information and very important and valuable data transferring over your network, as such you need to know both how to secure it and how to prevent any risks.

The 3 biggest risks I will assess:

# Loss of Service:

This is probably one of the biggest risks you could have to your business as the outcome from this happening could be loss of income, loss of customers and the loss of data.

## What can cause it?

* **Power Outages**

In this situation you would have no access to any of your services at the company and unless you have a trained a certified electrician on hand 24/7 would have to wait to get it fixed.

* **Defective Hardware**

This is something that can cause a massive amount of damage to your system in general depending on what fails. On the one side you have things like memory which when they fail is annoying, it doesn’t pose too much of a risk and can be fixed very quickly. Thus losses of any kind can be kept to a minimum however when something much larger fails like the CPU or hard drive of the system, you’re in for a world of costs and losses. This is because if something big like the hard drive fails and you don’t have policies and procedures in place to minimize the risks, you’re going to also lose any data that was stored on that hard drive.

* **Accidental Damage**

This is an easily preventable risk however you should always be aware of the threat that your own employees and clients pose to your network and systems.

* **ISP Problems**

ISP problem can causes a loss of service because you simply won’t be able to do things that rely on internet communication between your business and you clients.

* **Hacking**

Hacking is one of the most well-known threats, a hacker will generally go after targets of high value so they can sell it and make money. As such the data at risk here would be the file servers that store all your information. If that goes missing or if there is a breach you could not only face losses because of the loss of data but also because of law suits that companies would take out against you for losing their information.

* **Unidentified Access (Physical)**

This is the most basic of all attacks, the one where someone gets physical access and smashing something. This can also be one of the most costly (second to only hacking) as you not only lose all the data but you whole network infrastructure crumbles at which point your business grinds to a halt and you lose money each day it isn’t fixed.

# Loss of Business and Income:

## What can cause it?

* **Loss of Service**

As mentioned above, loss of service can also impact on the business in the form of a loss of business and income. This is most prevalent when you consider hacking as that could very well result in court cases against sports4u because of the breaking of the data protection act law.

* **Data Losses**

Every business runs on data, no matter how you look at it, the data you take in, process and pump out is the way in which you make money. So take that data away and you simply lose money.

* **Hacking**

I’ve mentioned it once already however hacking is a massive threat because of one thing, the Data Protection Act. The Data Protection Act has a principle within it that states you have to ensure adequate security of the data you are holding that is protected under this law. If a hacker gets into your system and steal that information, a case can be made against your company regarding whether or not you did adequately secure the data. If it is found that you didn’t then you can be facing massive legal bills and law cases from many of the clients you work with.

* **Stealing (Physical)**

Probably one of the oldest threats to businesses is physical stealing, the thing with physical stealing is that it is so easy to defend against in most situations and thus if it does happen to you and data is stolen as-well as hardware you again can face legal court cases which will cause a loss of service and a loss of money.

# Data Integrity:

Data integrity relates to how secure and safe the data you have stored on your network is. It doesn’t however just relate to how secure your security is that protects your network, data integrity can be effected by many things. The biggest threat to your data integrity comes in the form of hacking, hacking can come any many shapes and flavours however they all have the same end result which is to steal your data and either leak it or sell it online. The second huge threat to data integrity comes in a more physical form and is related to the storage device you would be using. In many cases vast quantities of data or stored on mechanical hard drives or solid state hard drives, the problem is that these things are physical and can essentially die or break. Losing power for example may result in corruptions which essentially makes your data useless as it has slight errors in it that make the remaining error free data essentially useless. Another problem that can arise may be that the hard drive itself simply dies, all HDD’s and SSD’s are subject to a certain life span as are all physical devices and as such can die and you again lose all your data.

# Ensuring Security:

So now you know all the big threats, how do you prevent them?

## Disaster Planning and Recovery Plans

A disaster and recovery plan is where you create a plan of action (or guide) that is to be followed in case of a disaster occurring to help minimise the risks to your overall system. These help by ensuring that you have something put in place to minimise the results of said disaster. These plans could literally include anything from ensuring a backup (more below) is on hand ready for the continuation of the company systems, to linking into an early warning system for things like earthquakes and floods to ensure all relevant precautions are taken just in case. No matter what plans you decide to implement they will all go towards minimising the fallout from any problem.

## ACL’s (Access Control Lists)

An access control list is a very important thing to be aware of and to have setup. The access control list is something you can take massive advantage of when using windows as its part of active directory. It essentially lets you set permissions for a specific user or group of users regarding how much access they have to certain folders, applications and resources. This is one of the most basic security steps to take as it ensures staff and other people on your network are not able to access things and thus edit things they’re not allowed or supposed to be editing.

## Backup and Restore Policies

A backup is by far the most basic and most useful thing to take advantage of on any system. What makes a backup when you have a network better though is your ability to store said backup in a location that isn’t in the sports4u premises. This helps minimise the risk to your backed up data as your whole server room could shut down or burn to a crisp and yet you still have your backed up data. This minimises any loss of service you might incur and also saves the business money as you’re not having to spend time and resources collecting all the data again.

## Password Policies

Password policies are where you have to create a password in a certain way that’s deemed by the system admins to be very secure. Normally this policy will state your password had to include an uppercase letter, a number and a special character. This is to help ensure that none of the employee passwords are easy to hack. Hackers will often use what is called a brute force attack to crack a password, this brute force attack simply goes through every single possible variation of characters that your password could be until it finds it. However it will often go through simpler passwords such as 1234567 and abcdefghi before it starts to try any more. This policy helps make it near impossible for hackers to break the password as easily as I just explained.

## Biometrics

Biometrics are often seen as futuristic however that’s very far from the truth. Biometrics have been used for several years now and are simply a form of identification that is either impossible or near impossible to replicate except from the person who’s identification it belongs to. The most common of all these identifications are finger print scanners, these are clever little devices that scan a person’s fingerprint and use that to determine who it is (seeing as everyone’s fingerprint is different). This helps secure your network even further and thus minimises many threats/risks.

## Encryption

Encryption is where you take your already stored data and completely muddle it up to make it look like complete gibberish. That is however for anyone except those that have the key (normally a complex maths equation) to put it all back in order again. This helps secure your data one step more as even if hackers where to get into your system or if someone physically stole the hard drives it is stored on, your data would still be safe as they’d not be able to decrypt it. This help minimise many risks which relate to data integrity as-well as many risks associated with hacking and stealing.

## Physical Security (CCTV)

CCTV is a form of security that simply has a camera pointed at the area you are trying to secure as-well as all entry points at all times. This helps prevent stealing however it also help prevent employees going into areas they’re not allowed in. If a member of staff or security guard see’s someone on the CCTV feed that is in an area that they’re not supposed to be in, an alarm can be raised to either have the person removed or ensure they’re not doing anything malicious. This will minimise risks that relate to the more physical side of security threats.

## Regular Updates and Patches

The operating system you use for your system and network will always be under a watchful eye from people trying to hack into it and people that would do something malicious. Furthermore any operating system is always open to the threat of viruses, malware and other such problems. While virus protection software and anti-malware may ensure your system stays safe, there is also another thing that can easily help protect your system on the operating system and even kernel level of your system. Those are both regular updates and to apply the latest patches, in many cases the creator of the operating system will be aware of threats and weaknesses far before anyone else may be and especially before sports4u may be aware of them, as such companies like Microsoft will release patches and updates to fix bugs, weaknesses and security threats within your system very quickly. That is why it’s always advised that you keep your system fully up to date and have a policy in place to ensure it does so.