John Doe  
1236 Travis Street  
 Trafalgar, Indiana  
574-101-1212

5/14/2024

Chris Nelson  
President  
Greenfield Properties  
123 Sophia Way  
Minneapolis, MN 55000

Dear Mr. Nelson:

Thank you for the opportunity to assist with your network planning for Greenfield Properties. I am writing to share my suggestions for setting up the IT network at Greenfield Properties' new building. With the merger of Bluegrass Rentals and Redstone Property Management into Greenfield Properties, it is important to create a strong and effective IT system that matches the company's goals.

To achieve this, I recommend moving from peer-to-peer LANs to client/server networking, which will help manage data and enhance security. Providing the right hardware, like PCs, tablets, and smartphones, to employees based on their roles will improve their work and connections. Using software for property management, accounting, HR, and IT management will make work smoother and improve teamwork. To protect important information, it's important to have good security measures like firewalls and antivirus software. A secure wireless network will help employees who work remotely or use mobile devices. Regularly backing up data and training employees will also make the network more reliable and secure.

These suggestions are aimed at helping Greenfield Properties reach its goals of having an efficient, secure, and always-available IT network. Don't hesitate to contact me if you have any further questions on my proposal below or need additional information.

Sincerely,

XXX

# **Introduction**

Greenfield Properties is combining Bluegrass Rentals and Redstone Property Management into a new company. This new company needs a strong IT network. This report gives suggestions for this network. It focuses on making the network easy to expand, efficient, and secure. We propose moving from old-style peer-to-peer networks to newer client/server networks. This change will improve how the network performs, keeps data safe, and helps employees work better. Our plan considers the different jobs at Greenfield Properties, making sure everyone has the right devices and tools to do their jobs well. This network upgrade will help Greenfield Properties succeed in its new building and future plans.

# **Network Infrastructure**

To effectively support Greenfield Properties' operations, I recommend setting up a client/server network. This network would consist of two switches connected to a router, with each wired device connected using Category 6 cables. Server functions would include Active Directory for user authentication, a file server for data sharing, a mail server for email management, a web server for hosting the company's website, and a database server for storing web server databases. Initially, cloud-based servers are suggested for easier management and cost savings. Network segmentation into four subnets for different device types, along with strategic deployment of multiple wireless access points, will ensure efficient network operations. Direct IP printing is proposed over a print server for simplicity and cost-effectiveness. Robust security measures, including physical security for IT equipment and software-based controls for infrastructure devices, will be implemented to protect against cyber threats. Regular maintenance schedules will also be established to keep the network secure, stable, and efficient.

# **Network Segmentation and Printing**

To make sure Greenfield Properties' network runs smoothly and stays secure, I suggest splitting it into four smaller parts called subnets. This means dividing the network based on the types of devices and how they're used. First, we'll have a subnet for computers connected with cables. This includes computers used by executives, office managers, human resources staff, and accounting personnel. This subnet will help manage the traffic efficiently and apply special security rules.Next, we'll have a subnet for devices that connect using Wi-Fi, like smartphones and tablets used by leasing agents, maintenance specialists, and others who need to move around. This separate subnet will keep Wi-Fi traffic isolated and make sure it runs smoothly.

Another subnet will be for important network devices like switches and routers. These devices will be in their own subnet to manage them separately and protect them with special security rules. Lastly, we'll have a subnet just for printers, both wired and wireless ones. This will make printing more efficient and help manage printer access. This segmentation will make it easier to manage the network, improve security, and apply different rules for each type of device. It will also help in fixing problems and keeping the network stable and safe.

# **Printing**

I think it would be a good idea to make printing easier and better at Greenfield Properties by putting all the printing services in one place. This means we would set up one main print server to control all the printing jobs. This server would manage print jobs, control who can use each printer, and keep everything organized. Right now, Greenfield Properties has 12 printers, and they plan to have 18 in the future. These printers are used for different things all over the company. We should set up one main print server to handle all the printers. This server would manage print jobs and make sure they get to the right printer. We'll set up a system where people have to prove who they are before they can print. This keeps documents safe and makes sure only the right people can see them. We'll also use special software to help us keep track of how much printing is happening and how much it costs. This can help us find ways to save money on printing. We could think about using fewer printers but putting them in the right places. This can save money and make things simpler. We'll set up printing so people can print from their phones or tablets. This can be really useful for people who move around a lot during the day. By using fewer printers and managing them better, we can save a lot of money on printing costs. With secure printing, we can make sure only the right people see printed documents. A central print server and print management software will make printing easier for everyone in the company. With a centralized system, people won't waste time trying to figure out which printer to use or where their print job went. Setting up a central printing system will not only make printing easier and more secure but also save money and time for Greenfield Properties.

# **Wi-Fi Networking**

For wi-fi, I recommend setting up a Wi-Fi network to provide reliable wireless internet access throughout the office building. This network will allow employees to connect to the internet and internal company resources using their smartphones, tablets, and other Wi-Fi-enabled devices. To ensure a strong and secure Wi-Fi network, it is important to install multiple access points strategically placed throughout the building. These access points will provide coverage to all areas of the office, minimizing dead zones and ensuring a consistent connection. To protect the network from unauthorized access, it is essential to use strong authentication methods, such as WPA2-Enterprise with 802.1X authentication. I order to maintain the security of company data only authorizrd devices are pemitted to connect to the network. Setting a Wi-Fi network will also improve employee productivity by allowing them to move freely around the office while still staying connected. This is particularly important for roles that require mobility, such as leasing agents and maintenance specialists. Setting up a Wi-Fi network at Greenfield Properties will provide employees with the flexibility and mobility they need to perform their roles effectively. It will also increase the overall efficiency of the company by ensuring a reliable and secure internet connection for all employees.

# **Security Measures**

To protect Greenfield Properties' new IT network, we need to use security measures. These measures are important to keep sensitive information safe and make sure the network runs smoothly. One important measure is using a firewall. A firewall helps control the flow of information in and out of the network. It stops unauthorized access and protects against cyber threats. Another important step is to use endpoint security. This means putting security on all devices like computers, tablets, and smartphones. This protects these devices from malware and other cyber threats. We also need to control who can access the network and sensitive information. This is called access control. Using strong authentication methods, like two-factor authentication, helps with this. It makes sure only the right people can access important information. It's also important to encrypt data. This means turning information into a code so that only authorized people can read it. We need to do this both when the data is being sent and when it's stored. Regular checks to make sure everything is safe and to find any weak points are also important. Lastly, we need to train employees about security. This includes teaching them about common security threats and how to protect sensitive information. With these security measures in place, Greenfield Properties can keep its IT network safe and secure.

### **Physical Security**

To make sure Greenfield Properties' IT network remains secure, we will implement three key security measures: access control, data protection, and network monitoring. The access Control is to control who can access the network, we will use usernames and passwords for user authentication. Additionally, we will employ role-based access control, ensuring employees only access resources necessary for their roles. This approach prevents unauthorized access and reduces the risk of data breaches for data protection. To safeguard data from unauthorized access, we will use encryption techniques. This process scrambles data, making it unreadable without the correct decryption key. This encryption will protect sensitive information, such as financial records and client data, from unauthorized users. Also, we will deploy network monitoring tools to continuously check network traffic for any suspicious activity. This proactive monitoring will help us find and deal with possible security problems right away, making security breaches have less impact.Setting these security measures will bring several benefits to Greenfield Properties. Firstly, it will protect their sensitive data, ensuring compliance with data protection regulations. Secondly, it will decrease the risk of costly data breaches, safeguarding their reputation and financial stability. Lastly, it will offer peace of mind to employees and clients, knowing their information is secure.

### **Infrastructure Access**

I propose a plan that focuses on secure and efficient access to network resources. This plan considers the diverse workforce, which includes executives, managers, leasing agents, and maintenance specialists. The proposed solution includes role-based access control (RBAC), where each employee's network access is based on their job role. To help maintain security, employees are granted access only to the resources required for their specific tasks. Additionally, a virtual private network (VPN) will be set up to allow remote employees, like the Public Relations and Social Media Manager, to securely access the network from outside the office. To add more extra layer of security, multi-factor authentication (MFA) will be implemented for accessing sensitive data or systems. This means employees will need to provide two or more verification factors to gain access, enhancing overall security. We will set up a special network just for visitors and clients to keep them separate from our main network. This will stop them from getting to any important information. We will also regularly check for any security problems and fix them to keep our network safe. Employees will have reliable and secure access to network resources, allowing them to work efficiently. This plan will help Greenfield Properties maintain a secure and efficient network environment for its employees.

### **Authentication**

Setting up a centralized authentication system at Greenfield Properties will greatly enhance network security and user accessibility. The proposed solution, including a centralized authentication server, single sign-on (SSO), multi-factor authentication (MFA), user account management, and access control, will address the current challenges and bring numerous benefits. These include improved security through MFA, a simplified user experience with SSO, efficient user account management, and better compliance with industry regulations and standards.

### **Lockout Policy**

To improve security for Greenfield Properties' IT network, I suggest setting up a network lockout policy. This policy will help protect the network from unauthorized access attempts and potential security breaches. Currently, there is no specific policy in place to handle repeated failed login attempts or unauthorized access to the network. The new policy will set a limit on how many times you can try to log in. If you exceed the attempt limit, your account will be locked for a specific period of time.It also involves including a provision for administrators to manually unlock accounts, setting up notifications for account lockouts, and conducting regular audits and reviews of the policy. By setting this lockout policy, we can make our network more secure by greatly lowering the chance of someone getting in without permission. It will also help Greenfield Properties meet compliance requirements related to network security and minimize disruptions for legitimate users by allowing account unlocking by administrators.

### 

### **Password Complexity Requirements**

To make Greenfield Properties' IT network more secure, I suggest implementing password complexity requirements for all users. Currently, there are no specific guidelines for password complexity, which can lead to weak passwords that are easily guessed or hacked. The proposed password complexity requirements include setting a minimum length of 8 characters, using a mix of letters (uppercase and lowercase), numbers, and special characters, avoiding common words or phrases, and enforcing regular password changes. You can also make a rule that locks an account if someone tries to log in and fails too many times. This can stop people from getting into the account without permission. This proposal can increase security, comply with security standards and regulations, and improve overall security awareness within the company. Implementing password complexity requirements is a simple yet effective way to enhance the security of the IT network.

### 

### **Firewall**

For a firewall, I suggest using a stateful network-based firewall. This type of firewall is smarter than traditional ones. It keeps track of active connections and can make better decisions about what traffic to allow or block. A stateful firewall is good at protecting against cyber threats like unauthorized access and malware. It checks incoming and outgoing traffic for suspicious activity. This helps prevent breaches and keeps sensitive information safe. It's important to protect all devices on the network, including printers. Each device should have its own software firewall. For Windows computers, the built-in Windows Defender Firewall is a good choice. Using these firewalls will help keep Greenfield Properties' network secure, reducing the risk of unauthorized access and potential vulnerabilities.

### 

### **Anti-Malware**

For Anti-Malware, I suggest using a strong anti-malware program to protect the company's computers from harmful software. Malware includes viruses, worms, and ransomware that can damage or steal information. The anti-malware program should have features like real-time scanning, which checks files and programs as they are used. It should also update automatically to stay protected against new threats. Another helpful feature is behavior analysis, which looks for suspicious actions that could be malware. This is also important to teach employees about safe internet use and how to avoid malware. The regular training can help them recognize and avoid dangerous websites and downloads.By using a good anti-malware program and educating employees, Greenfield Properties can reduce the risk of malware and keep their computers safe.