North Florida Cosmetology Institute

Information Technology Cyber Security Policy

Overview

1. OTS has been hired to ensure the security and integrity of the end client's network and data resulting from viruses, intrusion, hardware failure, or other factors within OTS control.
2. OTS uses tested and reliable vendor products to help deliver services and solutions to the end client.
3. The end client is responsible for ensuring their staff is properly trained on the company's policies and procedures regarding the proper delivery and use of the company's network and data by any federal, state or country laws and requirements. OTS does offer Security & Awareness Training for an additional fee.
4. OTS ensures all hardware used at the end client's site meets or exceeds the recommended specifications and requirement, as stated in the Managed Service Agreement. When any equipment no longer meets these standards, the end client agrees to replace the equipment to ensure it remains in compliance.
5. For an end user to gain access to the network, the request must be received from the owner or other authorized individuals assigned by the company.
6. To promote the security of OTS and the confidentiality of the data contained therein, access to OTS will be available only through approved workstations. End users shall commit to abide by the governing principles of OTS and adhere to the terms and conditions of the OTS End User Agreement.
7. An appropriate level of OTS access will be provided to those individuals that require access to perform their assigned duties on behalf of a OTS Partner Agency.
8. User logins are individual, and passwords are confidential. No individual should ever use, allow the use of, or share, in any format, a User ID and password that is not assigned to that individual.

Network Security Protection

Cyber-attacks and data breaches remain the biggest security threats to businesses. These attacks can take place from anywhere in the world and can have a massive impact and a magnitude of ramifications toward business and their consumers. The network outage to Sony on Christmas Day in 2014 and the data breach on Target in 2013 are only two examples of the type of attacks a business can suffer. While the following attacks focused on large corporations, the majority of small businesses don't realize they too can become a victim of these type of attacks. Hackers spend their time searching for weak infrastructures and use those to carry out even larger attacks at times. It is because of these increasing threats that OTS has chosen Unifi as their top vendor for network security. Unifi, an industry leader in security software and hardware, has proven to be an innovative and reliable security solution that helps ensure our client's networks remain secure. The solutions that Unifi provides include Unified Threat Management (UTM) Firewalls, Microsoft Email Spam Protection, Anti-Virus Protection, and Anti-Malware Protection as a standard requirement for our clients. Optional protection solutions include Email Archive, Anchor Email Encryption, Mobile Device Encryption, and Full Disk Encryption.

North Florida Cosmetology Institute

Information Technology Cyber Security Policy

Outsourced
Technology Solutions

- Unified Threat Management (UTM) Firewalls – With today’s increasing threats, the security services running within the firewall are essential to protecting the overall network. Without these services, many of today’s threats would have the ability to route themselves into the network. Unifi continues to advance their technological capabilities to inspect for and recognize these different threats and can prevent malicious activity by stopping the traffic the moment a threat is detected. It is this technology, along with the other web filtering services, that helps provide a complete security solution for the end client’s network.

- Anti-Virus/Malware Protection – Anti-virus solutions have been around for decades. However, not all solutions fully protect the local endpoints. Our Webroot Anti-Virus solution adds a deeper level of detection to keep threats off the local endpoints and works directly with the UTM Firewalls to monitor threats and help isolate them before they cause large outbreaks.

- Microsoft Email Spam Protection – Email is essential for running a business, but it also can be an easy way for hackers to gain access to the local network. By utilizing the Microsoft Email Spam Protection, we can quarantine questionable emails allowing the end user to review and release emails from senders they recognize. This solution works directly with the other Unifi solutions to ensure it continues to minimize the threats.

- Anchor Email Archive – As important as emails are, it can be time-consuming to search for an older email or to download a large number of emails. The email archive solution allows all emails to be kept securely in the cloud and has intelligent searching ability to help make email recovery simple and quick. Only the emails that the Email Spam Protection allows through will be archived, which helps to ensure the cloud archive remains secure.

- Microsoft Email Encryption – For businesses that need to send important information securely through email, the Microsoft Email Encryption product ensures those emails are encrypted from the point the email is sent until the expected recipient retrieves the email. If a hacker were to attempt to intercept the email the information they might be able to read would be extremely limited; helping to keep that message secure.

- Mobile Device Encryption – All the advancements in technology have allowed our users the ability to perform some of their work remotely via their mobile devices. However, there is always a chance these devices can be lost or stolen. The Microsoft Mobile Device Encryption helps to protect the data on these devices by encrypting the data and even gives OTS the ability to remotely wipe the device which greatly reduces the ability the hacker has to recover data.

- Full Disk Encryption – Many end users store confidential information locally on their computer or laptop and never think twice about its safety. If a local device is compromised, either by a cyber-attack or a physical act, that data would be easily compromised unless it was encrypted. The Bit Defender Full Disk Encryption allows specified local data to be encrypted and stored securely helping to keep it safe from any forms of attack.

- Dark Web Monitoring –

Security Assessments

To continuously monitor security threats to end client networks, OTS will perform security audits to ensure any new security threats are addressed. If critical threats are detected OTS will perform additional security audits as necessary until the threat is no longer of critical nature. These audits will include the review of:

- Microsoft Operating System patch versions to ensure all critical patches have been installed once approved by OTS

- Current software patching of known software application patch versions to ensure all software applications do not have any known vulnerabilities

- Anti-Virus protection definition versions to ensure all devices are receiving definition updates at minimum every 24 hours

- Anti-Virus system scans to ensure all devices have a full scan performed at least once a week

- Any available security and error logs

- Random assessment of end-user adherence to security policies. These assessments will include, but not limited to, how the end user handles vulnerable emails, unknown devices, phone calls requesting access to their devices, and other areas the OTS defines as potential violations to current security policies

- Age of current network passwords to ensure all passwords have been reset within the past 90 days

- UTM Firewall definition levels to ensure all services are running the latest approved versions and the review of all active and inactive services to ensure all necessary services are enabled and working properly

Physical Safeguards

Important physical safeguards are put in place to protect client privacy:

1. The location of all business computers must not be accessible to clients or other individual’s not employed or hired as a contractor by the client. In the event, this is necessary OTS must be notified of the requirements so additional safety precautions can be made.

2. The location of any network printers must remain in a secure location where only authorized persons have access.

3. Any computer screens that contain sensitive, confidential, client data, patient records, or other information that must remain private must be turned away from the view of any unauthorized users. If this does not provide enough protection, then privacy screen filters must be installed on the necessary devices to limit the visibility range.

North Florida Cosmetology Institute

Information Technology Cyber Security Policy

Outsourced
Technology Solutions

Requests for End User Network Access

To control network access, OTS requires all requests for end-user network access:

- Be received by the owner or authorized representative of the company
- Have the “Request to Add User” form completed to ensure all requirements are met
- Include any restrictions/access the end user must have

Password Policies

To assist in protecting the end client’s network, the following password policies have been established.

- Any temporary passwords must be changed upon first use. All user-specific passwords must be a minimum of 8 characters long and must contain a combination of letters and at least one number.
- End users will be prompted to change their network password every 90 days. All line of business software applications will need to be reset manually by the client, end user, or OTS staff
- End Users must immediately notify OTS if they have reason to believe that someone else has gained access to their password
- Five consecutive unsuccessful network login attempts will disable the User ID and will require the end user to contact OTS to have their password reset and account reactivated

Removing End User Network Access

When an end user needs an individual’s network access removed for whatever reason the following must be performed.

- The request must be received from the owner or authorized representative of the company
- The “Request to Remove User” form must be completed and submitted to OTS
- The date and time of when the user’s access is to be removed

<u>All requests to remove a user’s network access will require minimum 2-hour advance notice.</u>

Reporting Security Incidents

These security standards and policies to prevent—to the greatest degree possible—any security incidents. However, should a security incident occur, the following should be followed in reporting the incident:

1. Any end user who becomes aware of, or suspects, a compromise of any security and client privacy must immediately report that possible incident to OTS

2. In the event of a suspected security compromise OTS should complete an internal investigation. If the suspected compromise resulted from an end user's suspected or demonstrated noncompliance with the security policy, OTS will deactivate the end user's User ID until the internal investigation has been completed.

3. Following the internal investigation, OTS shall notify the end client of any information to substantiate incidents that may have resulted in a breach of the end client's security and client privacy. Whether or not a breach is definitively known to have occurred as a result of demonstrated noncompliance by an End User, the end client must inform OTS how to proceed with the end user's network access.

Backup & Disaster Recovery (BDR) Solution

To help minimize any potential data loss OTS strongly suggests using a Backup & Disaster Recovery (BDR) solution. This solution will perform a local, at a minimum hourly, backup of all client-approved servers and will transfer all backup images to the vendor’s SOC 2 Certified offsite storage facility to ensure an offsite image of the client’s data is available. This backup solution is intended for disaster recovery purposes only as the vendor has limits to their data retention policies. If a data archive solution is required, the end client must work with OTS to determine the best solution to address their needs. All local backups on the BDR solution will be retained for a minimum of 30 days, and all cloud backups will contain, at minimum, the most recent backup that was received by the offsite storage facility. A copy of the vendor’s SOC 2 Certification for their offsite storage facility is available upon written request to OTS.

Outsourced Technology Solutions

- 2450 Tim Gamble PL, 2nd floor
  Tallahassee, FL 32308
- **Phone:** 850-290-4466
- **Email:** support@outsourcemytech.com