Operational Procedures Study Guide for the CompTIA A+ Core Series Exam

General Information - Operational procedures generally tell you what to do in all sorts of circumstances, guiding you to the best practices for each situation. Below you will find an outline of the basic concepts in this area that occupies roughly one-fourth (23%) of the CompTIA A+ Core Series 1002 test. Nearly half of the questions in this domain are prefaced by a scenario and the headings for those areas are marked below with (*scenario*).

Documentation - It's vital to ensure that you read any required documentation before you begin working on any system. Documentation includes items such as **processes and procedures, network diagrams, knowledge base articles** (also known as **KBs**), and much more. It's also important to **document any fixes** that have been implemented so they can be referenced later. Another example of documentation includes **Safety Data Sheets or SDS** (formerly referred to as Material Safety Data Sheets or MSDS). The SDS outlines the procedures for disposing of hazardous materials. This should be referenced if there is a question about properly disposing of hazardous material. The SDS is administered by the **Occupational Safety and Health Administration (OSHA)** within the United States.

Network Topology Diagrams - Network topology diagrams are extremely helpful for performing any network **upgrades** or even to **troubleshoot** networking problems. The network topology diagrams will provide a visual representation of how the network is laid out, including both logical and physical information for the devices. **Visio** is a popular tool used when creating network diagrams.

Knowledge Base/Articles - A knowledge base is a repository of **information regarding an application or system**. When working on a system or troubleshooting an issue, individuals should first visit the systems knowledge base to see if a **solution** to their issue already exists.

Incident Documentation - You should adhere to the following order of operations when responding to any incident occurring on your computer network.

First response: The first step is the proper **confirmation** that an incident has happened, or is taking place. You should gather as much **information** as possible on the event, and **report** it through the proper authorized channels at the organization. These items will be outlined in a sound security policy.

Documentation: The next step is to document as much as possible. You can make use of **pictures**, **scratch notes**, or **event logs** to collect and assemble this information.

Chain of custody: Lastly, you want to make sure the **information you have is preserved**, especially in the event that information changes. Maintaining the **integrity of the information** is the most important step from this point forward. Any unaccounted changes could call into question the reliability of the information, making any work done since the first step useless.

Regulatory and Compliance Policy - When dealing with a networking environment, there are several regulations to keep in mind. These include: **electrical codes** for running high/low voltage cabling, **environmental codes** for disposing of chemicals or hardware, **fire prevention codes** requiring the specific use of dry or wet systems, and **building codes** that specify how cabling can be run through a building.

Acceptable Use Policy - An acceptable use policy (**AUP**) is a policy put in place by an organization that states which types of actions are acceptable to perform using their equipment. Many organizations implement acceptable use policies which state how employees are allowed to use their company-owned devices. Whenever accessing a public wi-fi, such as at a coffee shop like Starbucks™, you will have to acknowledge the AUP before getting access to the network.

Password Policy - Password policies state what is required when creating a password. **Weak passwords** can lead to data breaches and identity theft. To ensure that users create **strong passwords**, most password policies will include requirements for **length, complexity, and history**.

Inventory Management - Inventory management is the process of maintaining a database of which devices and systems exist within an organization. Inventory management is often done using a **third-party program** to keep track of devices within larger organizations.

Asset Tags - An asset tag is a method of inventory management. By adding asset tags to devices, it's easier to keep track of devices, including **who has the device** and **where they are located**.

Barcodes - Barcodes are types of asset tags that can be **easily scanned** to keep track of the devices.

Management Change (*scenario*) - Management Change (also called Change Management) is the process of addressing changes within an organization. Whenever a change is going to be made in an organization, **proper procedures** must be followed to ensure that any negative impact on the business or users is minimized.

Documented Business Processes - Any time a change is made within an organization, it's important to ensure that the business processes are documented. If the change is going to affect the current business processes, it should be evaluated and documented.

Purpose of the Change - Before making any changes, the purpose of the change must be documented. Typically, a **cost-benefit analysis** will also be done to see if the purpose of the change is worth the cost to implement and re-train staff on the new procedures.
Scope of the Change - Scope refers to the **extent of the changes** that will be made. While documenting the scope, it should outline exactly which items will be modified and changed through the project.
Risk Analysis - When making any changes within an environment, new risk will likely be introduced. Before making any changes in the environment, a risk analysis must be done. Upon defining the new risks which may arise, the organization must choose to **accept, mitigate, or avoid the risk**.
Plan for Change - Whenever implementing changes, it's also important to plan for changes that may arise throughout that process. **Before implementing** anything, there should be a plan in place for change.
End-User Acceptance - In order for a successful change, **all users must be on board** and prepared for the change. User acceptance testing is a common practice in which real users ensure that the change doesn't negatively affect their ability to perform tasks.
Change Board - A change advisory board (**CAB**) is made up of **individuals from various departments** throughout the organization. The CAB should also include high-level executives and stakeholders. This board will be responsible for **approving the changes** before they can be implemented. They will also be in charge of **overseeing** the project through to completion.
Backout Plan - With any change, there must be a backout plan in case unexpected issues arise. A backout plan would include a way to **revert to a previous version** of the system before the change was applied.
Document Changes - One of the most important aspects of the change management process is to document all changes as they are being made. This includes documenting **any new processes** that must be followed as a result of the change. **All challenges** that arise as a result of the change should also be documented.
Disaster Prevention and Recovery (*scenario*) - All organizations should have a **business continuity and disaster recovery (BCDR) plan** documented and in place. Disaster prevention and recovery refers to the ability to be able to bounce back after any type of disaster, such as a natural disaster or a cyber attack.
Backup and Recovery - Disaster can strike at any time, making it a requirement of information technology teams to have a full set of backups so they can quickly recover after an incident. Organizations should have **full backups** (which includes a backup of everything) and **incremental backups** (which includes only what has changed since the previous backup).
Image Level - An image-level backup creates a **full snapshot of the system** at a given point in time. This creates more of a full picture of the operating system and all the files included. This is a more complete option than file-level backups.
File Level - File-level backups are exactly what they sound like: **individual files and folders are selected** to be backed up.
Critical Applications - Critical applications should always be **a priority** when performing backups. File backups may not cut it when trying to backup critical applications. Microsoft Exchange servers and SQL servers will require additional work to back up above and beyond what file-level backups can offer.
Backup Testing - It's not enough to perform backups; the backups must also be tested. The test serves to **show that the backup files are not corrupt** and that they are backing up everything that would need to be restored in the event of a disaster. Backup tests should be **conducted regularly**.
UPS - If servers are not properly shut down, they can be damaged. This means that if there were to be a power outage, the server operating systems or applications may become corrupt. In order to prevent this type of scenario, systems should be plugged into an **uninterruptible power supply** (UPS). A UPS is an electrical device which provides power to a device in the event that the main power source fails.
Surge Protector - Surges occur when there is a **spike in voltage** or noise along the line. This can cause **damage to equipment** if the surge reaches the equipment. Surge protectors can counter this and send the excess voltage to the ground.
Cloud Storage vs. Local Storage Backups - Organizations will have to choose whether to use local storage backups (such as tape backups) or to back up to cloud storage. Some organizations may **also opt to have both** local and cloud storage as a second layer of disaster recovery. One drawback of cloud storage is that the data owner doesn't have full control over the data or where it is stored in the cloud.
Account Recovery Options - Account recovery **options will vary** depending on which type of account needs to be recovered. Many online accounts will have a "forgot your password?" option which will allow the user to have a password reset link emailed to them. If local accounts need to be recovered, Windows 10 has built-in features to recover lost passwords.

Common Safety Procedures - When dealing and working with computer components, keep safety **at the forefront** for both your and the device's sake. The following sections may be delivered as "scenario-based" questions in the exam environment, so you must be very comfortable with these topics.

Equipment Grounding - Equipment grounding is a way to transport any excess electrical discharge away from the component and into the electrical ground wiring. This is a safety mechanism that is included on all outlets, significantly **reducing the risk of electrical shock** should there be a fault within the system.

Proper Component Handling and Storage - You should be fully aware of how to handle and store the various components that can be affected by electrostatic discharge (ESD). The following items are the most common when managing ESD.

Antistatic Bags - These are used to store computer components when removing them from a computer and moving them around. This will ensure **minimal static buildup** and prevent damage.

ESD Straps - These are small wrist straps that can connect to an ESD mat or an ESD jacket for discharge to **reduce your electrostatic presence**.

ESD Mats - An ESD mat can either be a mat **you stand on** (floor mat) or a mat you **place the equipment on**. These ESD mats will reduce ESD risks, and some allow you to snap your ESD wristband into them for better protection.

Self-Grounding - Self-grounding means to remove or minimize the risk of ESD by taking premeditated **actions before working inside a computer**. This can be done by: working on hardwood tables, working on hard floors, wearing cotton clothing, and working in higher humidity environments. By gently running your hand across the bare metal of a computer case prior to reaching inside, you lessen the risk of ESD.

Toxic Waste Handling - You should be familiar with the proper procedures for handling several items that are considered toxic, including these:

Batteries - Newer technology batteries pose greater risks and should be **handled cautiously** when storing, charging, or disposing of. Improper charging can lead to fires and/or explosions that are difficult to extinguish with normal agents due to the chemical makeup of these batteries. Lithium batteries will get warm and might swell or leak if handled incorrectly while charging or transporting. You should wear **protective goggles** when working with these items. They should be taken to **waste facilities** for proper disposal due to chemical properties.

Toner - You should wear **protective goggles** and **air filters** when working with any toner cartridges. Toner appears in the cartridge and the printer as a dark, very fine powdery dust and is difficult to remove from clothing, skin, or other surfaces.

CRT - While not seen as often, cathode ray tube (CRT) monitors were the primary display units up until flat screen displays became mainstream. Some CRT screens contain **mercury**, **lead**, and **other materials** that can be hazardous to you and your surroundings. To power these tubes, they hold **a charge** that can be deadly when discharged. You should wear **protective goggles** when working with these items as well as **electrician gloves** in the event you need to open the case (no serviceable parts are inside). They should be taken to **waste facilities** for proper disposal due to the lead contained in the glass.

Cell Phones - Some states in the U.S. have made it illegal to throw cell phones in the trash, as they consider them hazardous material. This is likely due to the battery inside the smartphones. Instead of throwing the devices in the trash, the better option is to take them to an **electronic recycling facility**.

Tablets - Much like cell phones, tablets **should not be thrown in the trash**. Instead, they should be taken to an organization that recycles these devices.

Personal Safety - Be familiar with the following guidelines related to personal safety when dealing with computer components.

Disconnect Power Before Repairing a PC - All power sources should be disconnected prior to working inside a computer. Power supplies are typically replaced as a whole rather than in smaller individual parts. Normally there are **no serviceable parts inside** and therefore they should not be opened.

Remove Jewelry - All jewelry or anything dangling from your body should be removed. They can create a tangling hazard and/or cause a short circuit when they are near or come in contact with components.

Lifting Techniques - Always lift heavy equipment **using your legs** and not your back, or use multiple people to lift the object.

Weight Limitations - Use a **rolling cart** or something similar for overweight items when possible. Do not attempt to lift overweight items by yourself. **Weight limits are usually posted** on the outside of the boxing material. Observe a **"two-person rule"** when needed.

Electrical Fire Safety - For electrical fires, use specialized dry fire prevention or extinguishing chemicals, such as carbon dioxide. **Wet chemicals or water should never be used** on electrical fires.
Cable Management - Cabling should be **secured together** when run across spaces to prevent tripping, and should be covered if possible. There should never be any loose cabling to pose hazards to personnel or other equipment. Occupational Safety and Health Administration **(OSHA) regulations** should be verified and adhered to when running any cabling.
Safety Goggles - Use goggles when working with chemicals, batteries, or printer toner.
Air Filter Mask - To protect yourself from an environment where dust, smoke, or other air particles exist in the surrounding atmosphere, you should wear a special mask used to filter out these items.
Government Regulations - When dealing with a networking environment, there are several regulations to keep in mind. These include: electrical codes for running high/low voltage cabling, environmental codes for disposing of chemicals or hardware, fire prevention codes requiring the specific use of dry or wet systems, and building codes that specify how cabling can be run through a building.
Environmental Concerns - You should be able to quickly analyze and apply the proper controls for any possible environmental impacts. Some questions in this area will be of the scenario type.
SDS Documentation - The Safety Data Sheet or SDS (formerly referred to as Material Safety Data Sheet or MSDS) outlines the procedures **for disposing of hazardous materials**. This should be referenced if there is a question about properly disposing of hazardous material. The SDS is administered by the Occupational Safety and Health Administration (OSHA) within the United States. Copies are kept locally wherever there might be contact with hazardous materials.
Temperature, Humidity, and Ventilation - The temperature and humidity in the environment where components are stored should reflect the levels outlined in the SDS. For an electronic environment, it is usually best to balance the humidity as efficiently as possible to **avoid extreme condensation or static discharge**. It is also important to keep a closed-in area **well ventilated** so the room does not become too hot when the equipment is running.
Power Issues - Power issues can occur **anytime and anywhere**. These can range from total outages to flickers or surges, and can be devastating to equipment, data, and clients.
Battery Backup - An uninterruptible power supply (UPS) is used to maintain power to equipment in the event of a power outage or surge when all power can be lost or drop down below a certain threshold. The UPS will **automatically activate and provide power** for the connected equipment via batteries.
Surge Suppressor - A surge suppressor works by **checking for spikes in voltage** along the line. If a spike is detected, the surge protector **moves the excess power** to the ground and only allows the proper amount to be passed along to the connected devices.
Airborne Particles - You should be familiar with these two methods for countering airborne particles:
Enclosures - Your computer can be placed inside a special enclosure if it is in a location where there are a lot of particles in the air, such as smoke or dust. These are typically found in **factory or plant locations**.
Air Filters/Masks - To protect yourself from an environment **where dust, smoke, or other air particles exist** in the surrounding atmosphere, you should wear a special mask used to filter out these items.
Dust and Debris - You should be familiar with these two methods for cleaning dust and debris in a computing environment:
Compressed Air - Compressed air can be used to clean out the inside of computer equipment, as well as printers or other devices. It is better to **use natural compressed air** versus any chemical-based compressed material.
Vacuums - Only specialized anti-static vacuums should be used in electronic environments. These vacuums can help reduce the risk of a static discharge or damage to the component.
Government Regulations - You should be aware of any local regulations regarding the industry in which you operate, such as disposal procedures or safety implications. In addition, the Safety Data Sheet (SDS) outlines how to dispose of hazardous materials. This should be referenced if there is a question about how to properly dispose of any hazardous material or if you simply require more information about the item in question. The SDS is administered by the Occupational Safety and Health Administration (OSHA) within the United States. Environmental concerns are administered nationally by the **U.S. Environmental Protection Agency (EPA)**.
Regulation of Technology Use
Licensing/DRM/EULA - For this exam, you should be very comfortable with the many types of licensing arrangements available today, including **digital rights management (DRM)** and **end user licensing agreements (EULA)** that stipulate how the software can be used.

Open Source vs. Commercial License - An *open source license* means that the software's source code is freely available to the public. This means the software can be modified and recreated if desired by the end user. A *commercial license* is usually closed source, meaning the source code is not available to the general public.
Personal License vs. Enterprise Licenses - A *personal license* is granted only to one end user for recreational purposes. At times, costly commercial software will license its product for non-commercial use to an individual or student, and this is intended for personal use only. *Enterprise licenses* are intended for business use, typically by larger organizations, and are a form of paid commercial software licensed to the company for a certain number of users.
Incident Response - You should adhere to the following order of operations when responding to any incident occurring on your computer network.
First Response - The first step is the proper confirmation that an incident has happened, or is taking place. You should gather as much information as possible on the event and report it through the proper authorized channels at the organization. These items will be outlined in a sound security policy.
Identify— We have tasks to complete every day. While completing these, if something looks different, then you have just *identified* something. By using **checklists** and following these checklists as a daily task, you are more likely to identify an incident long before it possibly affects the system.
Report— Once confirmed, ensure others in your chain of command are notified that an incident has occured. Document the person and title you informed as well as the time they were informed. Having a **standard report form** will assist in this procedure.
Preserve— To obtain a full incident overview, preservation is paramount. Ensuring that the **evidence remains intact** and undisturbed will preserve the incident for investigation.
Documentation
The next step is to document as much as possible and continue documentation as changes are made to the incident. You can make use of pictures, scratch notes, or event logs to collect and assemble this information.
Chain of Custody - Lastly, you want to make sure the information you have is preserved, especially in the event that information changes. Maintaining the integrity of the information is the most important step from this point forward. Any unaccounted changes could call into question the reliability of the information, making any work done since the first step useless.
Tracking of evidence— Evidence of an incident can be vital to proving the who, what, when, and how of the incident. Ensuring this evidence is maintained while the investigation is being completed should be conducted with evidence trackers and chain of custody logs. These can be generic forms or be generated internally, but should be started as soon as the documentation begins.
Documenting progress— During the investigation phase of the incident and all during the process, everything must be documented to maintain the incident. Any slight infraction can lead to "tainted" evidence and the investigation being sidelined.
Regulated Data - Within the scope of information technology is data that must be held to a higher standard than that of other data. In cases of *regulated data*, the federal government has developed standards as to the handling of this data.
PII— **Personally Identifiable Information**: This is information that can be used as a means to identify employees within an organization, such as Social Security numbers and addresses. This information should remain very secure, and there should be clearly defined policies stating who can access it.
PCI— **Payment Card Industry**: Security standards that ensure all companies that accept, process, store, or transmit credit card information maintain the security of such information.
GDPR— **General Data Protection Regulation**: Regulations based on data protection and privacy within the European Union.
PHI— **Protected Health Information**: Information relating to health information of the person stored, transmitted or maintained in electronic or other forms. Subject to state and federal privacy and security rules, including the Health Insurance Portability and Accountability Act (HIPAA).
Policies and Security Best Practices
Most of these policies, including end user policies, were created to best protect the organization's network and should all be followed. Many items that a company may disallow or restrict can pose significant security risks to the computer infrastructure. This makes it **very important that all policies are followed**, and that all employees from entry level to CEO are educated on security best practices.
Communication Techniques and Professionalism (*scenario*)

Those working in IT should be aware of the following concepts in order to use proper communication techniques and professionalism.

Language - You should always **use proper language** when speaking with a customer or client. The majority of end users are not very technology-oriented, so you should **avoid tech slang and acronyms**, breaking down the meaning of all terms used in a constructive manner. We sometimes get caught up in technical language and should always avoid "tech speak" or talking above the client's head.

Attitude - You should display a **great attitude** when dealing with technical issues that may be complex. Use all cases as lessons to acquire more knowledge about technology. Also, **be confident** when discussing technical issues with end users. Be aware that it is more about being able to *find* the right answer than having all the answers memorized. Regardless of the situation, **remain positive** and project confidence in your work. Customers know that you don't know everything, but you should avoid giving the impression that you are unsure of the procedure to find a solution.

Listening - When discussing issues with a customer, **actively listen** and **take notes** when appropriate. Customers should never have to repeat themselves because you did not write down key details. Additionally, **never interrupt** customers while they are giving you information. Let them tell you their story in full and then you can respond with follow-up questions if needed. Remember, always listen to understand what the customer is saying.

Sensitivity - You should always **greet users with respect** and **use their proper professional titles** when addressing them. If someone is a director, don't refer to them as a manager—not in person, in support documentation, or on the phone with one of your colleagues. This is an easy way to offend someone quickly. Remember that some people have different cultural backgrounds than others, so you should always **remain culturally sensitive** to their requests.

Punctuality - Punctuality is extremely important as an IT professional. Often, end users have meetings or their own work to complete and you are seen as the piece that is holding them up. Always arrive on time for pre-scheduled appointments and always **contact clients if there will be any delay** relating to the service. If anything keeps you from arriving at the client's location on time, notify the customer of your situation beforehand and give them an **estimated arrival time**.

Distractions - While working with clients, be sure to avoid all types of distractions. This includes text messages, phone calls, or simply having conversations with other colleagues. You never want to give the impression that the end user does not have 100% of your attention. Their technical problem must appear to be the number one priority when you are in their presence, even though that may not be the case. Listed below are some, but not all, of the distractions that should be avoided at all costs.

- Personal calls
- Texting/social media sites
- Talking to coworkers while with customers
- Personal interruptions

Difficult Situations and Customers - When handling difficult situations or customers, be sure to do the following:

Do not argue— Arguing with customers will not get the result that either of you are hoping to achieve. **Try not to become defensive** when speaking with a client, even if they seem like they are being unreasonable. Letting the customer know that you understand their frustration will help them to feel confident that you can help them solve the problem.

Avoid dismissing customer problems— Try to avoid dismissing the customer's problems or issues. Even though an issue may not seem like a big deal to you, it may be very important to them.

Avoid being judgmental— Avoid being judgemental when working with clients. Something that may seem easy and self-explanatory to you could be quite challenging and difficult to them. It's important to keep in mind that not everyone is tech-savvy.

Clarify customer statements— **Ask questions** to ascertain the root of the problem. When a customer tells you his or her story, restate what you believe the problem to be to confirm an understanding through the verification process.

Maintain privacy— **Never use social media** as an outlet to vent about a particular customer or experience. Things on the Internet typically stay there forever and this could portray you or your company in a bad light.

Meeting Customer Expectations

When working on a client issue, always be prepared to **set initial expectations** with the promise of action to follow. Keep the customer informed of any changes, but make sure all promises are kept in a timely manner.

Options— If possible, always give the customer **multiple options and alternatives**. Even if you prefer one way, remember this is the end user's equipment and they should be given the opportunity to weigh their options.

Documentation— Keep up-to-date documentation and **provide this to the customer when the service is complete**. Customers will feel more at ease if they can review what work was performed on their PC, as they will know exactly how their money was spent on the repair.
Follow up— When the device has been returned to the customer after service, follow up at a later time to **verify satisfaction**. This is one of the most important steps in having repeat customers, as they will feel like you genuinely care about the service.
Privacy of Records - When working on a customer's issue, use best practices in handling their data. This is the customer's private information, and directly accessing this data is usually not required to complete a repair. It is your duty to keep that information safe and secure for as long as it's in your possession.
Scripting - Scripting can be used to automate IT management processes. It is important to be familiar with all of these concepts.
Script File Types - You should be able to identify the basic types of script files.
.bat— A batch file is a series of commands to be run by the Windows operating system stored in a plain text file.
.ps1— A .ps1 file is used to run scripts in Powershell.
.vbs—A .vbs file contains lines of codes in the Visual Basic programming language which are encoded in plain text format.
.sh— A .sh file is like the batch files of Windows but they can be executed in Linux or Unix.
.py— A .py script is a script written in the Python programming language.
.js—. A .js file is a script written in JavaScript.
Environment Variables - An environment variable is a dynamic-named value that can affect the way running processes act on a computer. **Shell scripts** and **batch files** use environment variables to communicate data and preferences to child processes.
Comment Syntax - Adding comments to your scripts can help both you and individuals who view your script in the future understand what you were trying to accomplish. The syntax used to add comments will vary depending on the programming language, but often a / or // will denote a comment.
Basic Script Constructs
Basic loops— A basic loop structure encloses a sequence of statements in between the loop and end loop statements. With each iteration, the sequence of statements is executed and then control resumes at the top of the loop.
Variables—- A variable is a symbolic name for a piece of memory to which we can assign values, and read and manipulate its contents.
Basic Data Types
You should be aware of the following data types.
Integers— An integer is a whole number (not a fraction) that can be positive, negative, or zero.
Strings—A string is essentially a string of characters used to represent text rather than numbers.
Remote Access Technologies (*scenario*)
Accessing devices remotely is a major part of troubleshooting issues. Let's look at a few remote access technologies.
RDP - RDP, or **remote desktop protocol**, is a Microsoft proprietary technology for remotely accessing Windows computers. RDP provides a user **with a graphical interface** to connect to another computer over a network connection.
Telnet - Telnet is a protocol which creates a **two-way communication connection** between computers over a network connection (via the Internet or local area network). Telnet has **no graphical user interface** like RDP does; it is strictly **terminal-based**. Telnet typically operates on **port 23**.
SSH - Telnet is not very secure, so SSH has pretty much replaced telnet for communication over the network. SSH is also **a terminal-based program** with **no graphical interface**. SSH operates on **port 22**.
Third-Party Tools - Many third-party tools can provide a quick, reliable, and efficient way to connect to computers.
Screen Share Feature - One common feature that most third-party remote access tools include is screen sharing. A screen sharing feature allows a technician to **view the client's screen** and see exactly what they are seeing.
File Share - File sharing is another feature that comes in handy when working on a remote computer. File sharing allows for **files from one device to be moved** to the other remote device.
Security Considerations - When considering which remote access option to use, it's vital to consider the security ramifications. For example, leaving a telnet port open can create security vulnerabilities. When using third-party tools, it's best to ensure they offer **multi-factor authentication** so that only legitimate users can gain access to the devices remotely.