

KENNEDY SECONDARY SCHOOL-ENTEBBE

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

840/1 (Theory Paper)

Senior Four
TERM ONE 2025

EXPECTED RESPONSES

ITEM 1 (A).

The "No bootable device found" error indicates that your computer is unable to locate a device containing a valid operating system to start up. Several factors can contribute to this issue:

1. **Incorrect Boot Order:** If the BIOS/UEFI settings prioritize a device without an operating system, the system won't find a bootable device.
2. **Disconnected or Faulty Hard Drive:** A loose or malfunctioning hard drive can prevent the system from detecting it as a bootable device.
3. **Corrupted Master Boot Record (MBR):** The MBR contains essential boot information. If it's damaged, the system may not boot properly.
4. **Damaged Operating System Partition:** If the partition containing the operating system is corrupted or deleted, the system won't find a bootable device.
5. **External Devices Interfering:** Connected USB drives, CDs, or DVDs can interfere with the boot process if they contain bootable media.

ITEM 1 (B).

John can determine whether his hard drive is failing which involves observing specific symptoms and performing diagnostic tests. Here's how he can assess his hard drive's health:

1. Monitor for Warning Signs:

Be alert to the following indicators of potential hard drive failure:

- **Unusual Noises:** Clicking, grinding, or whirring sounds can suggest mechanical issues.
- **Frequent System Crashes or Freezes:** Unexpected shutdowns or system freezes may point to hard drive problems.
- **Slow Performance:** Significant delays in accessing files or booting up can be a sign of a failing drive.
- **Corrupted or Missing Files:** Difficulty opening files, missing data, or error messages when accessing files can indicate disk issues.

2. Utilize Built-in Diagnostic Tools:

- **Windows Check Disk Utility:**
 - Open Command Prompt as an administrator.
 - Type `chkdsk C: /f` (replace 'C:' with your drive letter) and press Enter.
 - This command checks for file system errors and attempts to fix them.
- **MacOS Disk Utility:**

- Navigate to Applications > Utilities > Disk Utility.
- Select your hard drive and click on "First Aid" to check and repair disk errors.

3. Employ Third-Party Diagnostic Software:

Specialized tools can provide a more detailed analysis of your hard drive's health:

- **Hard Disk Sentinel:** Monitors hard drive health and provides detailed reports.
- **CrystalDiskInfo:** Offers a user-friendly interface to view S.M.A.R.T. data and health status.

4. Check S.M.A.R.T. Status:

Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) can indicate potential failures:

- Use tools like CrystalDiskInfo to view S.M.A.R.T. attributes.
- Look for attributes like "Reallocated Sectors Count" or "Spin Retry Count," which can signal issues.

ITEM 1 (C).

Below are the steps John should take to resolve, restore and recover his data.

1. **Check Boot Order:**
 - Restart your computer and enter the BIOS/UEFI settings (commonly by pressing keys like F2, Del, or Esc during startup).
 - Navigate to the Boot menu and ensure your primary hard drive is set as the first boot device.
2. **Inspect Hardware Connections:**
 - Power off your computer and disconnect all external devices.
 - Open the case and verify that the hard drive is securely connected to the motherboard and power supply.
3. **Reset BIOS/UEFI Settings:**
 - In the BIOS/UEFI, look for an option to reset to default settings.
 - Save and exit to see if the issue persists.
4. **Check for External Devices:**
 - Disconnect all USB drives, CDs, DVDs, and other external devices.
 - Restart the computer to see if it boots correctly.
5. **Repair the Master Boot Record (MBR):**
 - If you have a Windows installation disk or recovery drive, boot from it.
 - Select "Repair your computer," then navigate to "Troubleshoot" > "Advanced options" > "Command Prompt."
 - In the Command Prompt, type bootrec /fixmbr and press Enter.

Conclusion:

If these steps don't resolve the issue, it might indicate a hardware failure or a more complex software problem. In such cases, consulting a professional technician is advisable.

ITEM 2 (A).

Introduction:

To reduce strain and discomfort during computer use, it's essential to set up your workstation ergonomically. Here are key adjustments to consider:

1. Chair and Seating Position:

- **Seat Height:** Adjust your chair so your feet rest flat on the floor, with thighs parallel to the ground.
- **Back Support:** Ensure the chair supports the natural curve of your lower back to maintain proper posture.
- **Armrests:** Position armrests so your upper arms hang naturally at your sides, with forearms parallel to the floor.

2. Desk and Monitor Setup:

- **Monitor Position:** Place the monitor directly in front of you, with the top of the screen at or just below eye level, about an arm's length away.
- **Keyboard and Mouse:** Keep the keyboard and mouse close, allowing your wrists to remain straight and hands at or below elbow level.

3. Posture and Movement:

- **Neutral Posture:** Maintain a relaxed, neutral posture with shoulders back, elbows close to your body, and wrists straight.
- **Breaks and Movement:** Take short breaks every 30-60 minutes to stand, stretch, and walk around to alleviate muscle tension.

4. Lighting and Glare:

- **Lighting:** Use ambient lighting to reduce glare on the screen. Position your monitor perpendicular to windows to minimize reflections.
- **Screen Brightness:** Adjust screen brightness to match ambient lighting and reduce eye strain.

5. Equipment and Accessories:

- **Ergonomic Tools:** Consider using ergonomic keyboards and mice that promote natural hand positions.
- **Standing Desks:** Alternating between sitting and standing can reduce strain. Standing desk converters allow for easy transitions.

Conclusion:

Implementing these ergonomic adjustments can significantly enhance comfort and reduce the risk of strain during computer use.

ITEM 2 (B).

Introduction:

Poor ergonomics in an Information and Communication Technology (ICT) environment can lead to several health issues, primarily affecting the musculoskeletal and visual systems. Key problems include:

- 1. Musculoskeletal Disorders (MSDs):** Prolonged use of computers without proper ergonomic setup can result in MSDs, causing pain and discomfort in the back, neck, shoulders, and wrists. These disorders often stem from repetitive movements, awkward postures, and sustained positions.
- 2. Eye Strain (Computer Vision Syndrome):** Extended screen time can lead to eye strain, characterized by redness, dryness, and discomfort. This condition is exacerbated by poor lighting and improper screen positioning.
- 3. Repetitive Strain Injuries (RSIs):** Repetitive motions, such as typing or using a mouse, can cause RSIs, leading to inflammation and pain in the tendons and muscles. Conditions like carpal tunnel syndrome are common examples.
- 4. Headaches and Migraines:** Improper ergonomics can contribute to headaches and migraines, often due to muscle tension in the neck and shoulders or eye strain from poor screen setup.
- 5. Poor Posture-Related Issues:** Sitting for extended periods without proper support can lead to poor posture, resulting in back and neck pain. This is often referred to as "dead butt syndrome," where prolonged sitting leads to muscle weakness and discomfort.
- 6. Fatigue:** Inadequate ergonomic setups can cause fatigue due to muscle strain and discomfort, leading to decreased productivity and increased risk of errors.
- 7. Decreased Circulation:** Sitting in one position for too long can impair circulation, leading to numbness, tingling, and increased risk of deep vein thrombosis.
- 8. Mental Health Effects:** Chronic discomfort and pain from poor ergonomics can contribute to stress, anxiety, and depression, affecting overall well-being.

Conclusion:

To mitigate these health risks, it's essential to maintain an ergonomic workspace by adjusting chair height, ensuring proper screen positioning, taking regular breaks, and practicing good posture.

ITEM 3 (A).

Improper disposal of electronic waste (e-waste) poses significant environmental risks, including:

- **Soil Contamination:** Toxic substances such as lead, mercury, and cadmium can leach into the soil from discarded electronics, adversely affecting plant life and entering the food chain.

- **Water Pollution:** When e-waste is improperly disposed of, hazardous materials can seep into groundwater, contaminating water sources and harming aquatic ecosystems.
- **Air Pollution:** Open burning of e-waste releases toxic fumes, including dioxins and furans, which can travel significant distances, contaminating air quality and posing health risks to distant communities.
- **Ecosystem Degradation:** The release of toxic chemicals from e-waste can lead to ecosystem degradation, loss of biodiversity, and the disruption of delicate ecological balances.
- **Resource Wastage:** Improper disposal results in the loss of valuable materials like gold, copper, and silver, which could otherwise be recovered and reused, contributing to resource conservation.
- To mitigate these environmental risks, it's essential to dispose of e-waste responsibly through certified recycling programs that ensure safe handling and recovery of valuable materials.
- E-waste negatively impacts the soil.
- E-waste damage the soil, as e-waste breaks down, it releases toxic heavy metals like lead, arsenic and cadmium. When these toxins reach into the soil, they influence the plants and trees that are growing from this soil.
- When E-waste toxins enter the soil, they can also enter the human food supply which can lead to birth defects as well as other health complications.
- E-waste negatively impacts the water.
- E-waste toxins enter the ground water, this ground water like ponds and lakes many animals rely on them thus toxins can make these animals sick.
- When e-waste toxins enter the ground water, people who rely on and use the water can become sick.
- E-waste negatively impacts the air.
- Whenever e-waste is burnt, they release hydrocarbons in the atmosphere, which pollutes the air that many animals and humans rely on. Thus humans and animals become sick.
- The hydrocarbons released into the atmosphere whenever e-waste is burnt lead to global warming.

Conclusion:

To mitigate these environmental risks, it's essential to dispose of e-waste responsibly through certified recycling programs that ensure safe handling and recovery of valuable materials.

ITEM 3 (B).

Introduction:

E-waste management companies play a crucial role in mitigating environmental impacts associated with electronic waste. To handle and recycle e-waste responsibly, they should adhere to the following best practices:

- **Collection and Sorting:** Implement organized collection systems to gather e-waste from various sources. Sorting the collected items by type and material is essential for efficient recycling.
- **Dismantling and Separation:** Carefully disassemble electronic devices to separate hazardous components (such as batteries and capacitors) from recyclable materials like metals and plastics. This step prevents the release of toxic substances and facilitates material recovery.

- **Recycling Processes:** Utilize specialized equipment to process materials extracted from e-waste. Techniques like shredding, size reduction, and chemical treatments can recover valuable metals and ensure safe disposal of hazardous substances.
- **Data Destruction:** Implement secure data destruction methods to protect sensitive information on electronic devices before recycling. This step is vital for maintaining data privacy and security.
- **Public Education and Awareness:** Educate the public about the importance of proper e-waste disposal and recycling. Encouraging responsible consumer behavior can increase the volume of e-waste directed to certified recycling facilities.
- Sensitizing people on cutting down on purchases. This should be done by informing people to avoid buying many electronic equipment that they don't badly need to use.
- Make use of clouds, people should store and manage all their data using servers.
- Donating older products, older electronic equipment handled well and still able to work should not be discarded once new equipment are bought, so should be donated.
- Making repairs, they can repair most electronic equipment to work again instead of disposing of them.

Conclusion:

By implementing these practices, e-waste management companies can significantly reduce environmental pollution, conserve valuable resources, and promote sustainable development.

ITEM 3 (C).

Introduction:

ICT (Information and Communication Technology) companies must follow strict regulations when disposing of hazardous materials, including batteries, to ensure environmental protection and public safety. The regulations they need to adhere to depend on the country or region they are operating in, but generally, the following frameworks and guidelines apply:

Key Principles for Disposal of Hazardous Materials (Batteries):

- **Proper Collection:** Companies must ensure that batteries are collected and separated from general waste streams.
- **Recycling:** Batteries should be sent to certified recycling facilities where hazardous materials can be safely recovered and reused, reducing the environmental impact.
- **Labeling and Communication:** Batteries containing hazardous materials must be clearly labeled, and companies should provide information to consumers on how to dispose of or recycle them.
- **Training and Compliance:** ICT companies must train employees to handle hazardous materials safely, follow disposal regulations, and keep records for compliance.

Conclusion:

By adhering to these regulations, ICT companies can reduce their environmental impact and avoid legal consequences related to improper disposal. It is important for these companies to regularly check the evolving legal landscape in their operating regions to stay compliant with current environmental standards.

ITEM 3 (C)

Introduction:

In Uganda, ICT companies are required to follow several key regulations and guidelines when disposing of hazardous materials, including batteries. While Uganda may not have a highly detailed or specific set of regulations for every type of hazardous material disposal, the country has adopted broader environmental laws and international frameworks to ensure safe disposal and management. Here are the key regulations ICT companies must follow:

1. The National Environment Act (NEA)

- **National Environment Management Authority (NEMA):** The National Environment Act is Uganda's primary environmental law, and it empowers the National Environment Management Authority (NEMA) to regulate and enforce environmental standards. The NEA provides guidelines for the disposal of hazardous waste, including electronic waste (e-waste) and batteries.
 - NEMA is responsible for ensuring that ICT companies comply with environmental protection standards, including waste management.
 - ICT companies must submit e-waste management plans, including how they will dispose of hazardous materials like batteries in an environmentally responsible manner.

2. The National Environment (Waste Management) Regulations, 2020

- These regulations aim to address waste management in Uganda, including the disposal of hazardous waste such as batteries.
 - **E-Waste:** This includes ICT equipment and batteries that contain hazardous materials such as mercury, lead, and cadmium. ICT companies must ensure these materials are properly managed and disposed of by authorized waste handlers.
 - **Waste Segregation:** Companies are expected to segregate hazardous materials from regular waste and handle them with care. Batteries must be treated as hazardous waste due to their toxic components.

3. The Uganda National Policy for E-Waste Management

- This policy addresses the growing problem of electronic waste in Uganda and sets out guidelines for the collection, recycling, and disposal of e-waste.
- While not strictly enforceable, this policy encourages companies to adopt responsible e-waste management practices, which include battery disposal. It promotes recycling and reuse of valuable materials from electronic devices, including ICT batteries, to reduce environmental pollution.

4. The Environmental Impact Assessment (EIA) Guidelines

- Under the National Environment Act, companies in Uganda are required to conduct Environmental Impact Assessments (EIA) for projects that may result in significant environmental harm, including the disposal of hazardous waste.

- ICT companies may be required to conduct EIAs if their activities involve significant amounts of hazardous waste disposal (e.g., when disposing of old batteries in bulk), and they must assess and mitigate potential environmental impacts.

5. The Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal

- Uganda is a signatory to the **Basel Convention**, an international treaty that governs the cross-border movement and disposal of hazardous waste, including batteries.
- The convention emphasizes environmentally sound management of hazardous materials, meaning that ICT companies must ensure that their disposal methods (such as shipping e-waste or batteries to recycling centers) meet international standards for protecting the environment and human health.

6. The Kampala City Ordinance on Waste Management

- In cities like Kampala, local ordinances may provide additional regulations regarding waste management, including hazardous waste like batteries.
- These ordinances typically require businesses to work with certified waste disposal and recycling companies to ensure safe disposal and proper management of toxic materials in urban environments.

7. The Uganda National Bureau of Standards (UNBS)

- The Uganda National Bureau of Standards (UNBS) may establish regulations around the importation and handling of batteries to ensure they comply with national safety and environmental standards. These standards help guide companies in ensuring they meet acceptable criteria for the disposal of hazardous materials.

Key Steps for ICT Companies in Uganda When Disposing of Hazardous Materials Like Batteries:

- **Compliance with NEMA Guidelines:** Ensure that disposal methods follow the guidelines set by NEMA for hazardous waste management.
- **E-Waste Management:** Adopt responsible practices for handling and disposing of e-waste, including batteries. Companies should work with certified waste management companies that specialize in the recycling of electronic components.
- **Proper Segregation and Labeling:** Batteries should be clearly identified and segregated from regular waste. ICT companies must ensure that employees and consumers know how to handle and dispose of batteries properly.
- **Work with Certified Recyclers:** Only work with licensed and certified recycling facilities that can safely handle and recycle hazardous materials.
- **Environmental Reporting:** Some companies may need to report their waste management practices to NEMA or local authorities. It is important to maintain records of hazardous waste disposal, including battery recycling.

Conclusion:

By adhering to these regulations, ICT companies in Uganda can help protect the environment, avoid penalties, and contribute to sustainable waste management practices. It's also important to stay updated on local regulations, as they can change over time.

ITEM 4 (FROM THE ONLINE GUIDE BY MR. KAKURU BENARD)

ITEM 5 (A).

If you've forgotten your job application account password, here are the general steps you can take to recover it:

1. Look for a "Forgot Password" or "Reset Password" Option

Most job application platforms provide a way to recover your password directly from the login page. Follow these steps:

- Go to the **login page** of the job application website.
- Look for a link or button that says "**Forgot Password?**", "**Reset Password**", or something similar.
- Click on this link, and it will guide you through the recovery process.

2. Enter Your Email Address or Username

- You will likely be prompted to enter the email address or username associated with your account. Make sure to enter the correct information you used when creating the account.
- If you've used multiple emails, try the one you most likely registered with.

3. Check Your Email for a Reset Link

- After submitting your email address or username, the platform will typically send a password reset link to your email.
- **Check your inbox** for an email from the job application site. Be sure to also check your **Spam or Junk** folder in case the email was filtered.
- Click on the **reset link** provided in the email.

4. Create a New Password

- After clicking the reset link, you will be redirected to a page where you can enter a **new password**.
- Choose a **strong password** that you haven't used recently for this account. Some sites may have specific requirements, like a minimum length or a mix of characters.
- Enter the password, and confirm it by typing it again.

5. Log In with Your New Password

- Once the password is reset, you should be able to log in with your **new password**.
- Make sure to save it somewhere safe or use a password manager to help you remember it in the future.

6. Contact Support (if Needed)

- If you're unable to reset your password (e.g., if you no longer have access to the email address you registered with or you're not receiving the reset email), look for a **customer support** or **helpdesk** contact option.
- Explain your issue and provide any necessary account details (such as your username, email address, or other identifying information) to verify your identity.
- Some platforms may also offer recovery options through **SMS** or **security questions**.

Additional Tips:

- **Update your email:** If you realize you don't have access to the email account tied to your job application account, contact the platform's support to change your registered email.
- **Use Two-Factor Authentication (2FA):** If the site supports it, set up **2FA** to secure your account and make recovery easier in the future.
- **Save Your Passwords:** Consider using a **password manager** to store and manage your passwords securely, making it easier to retrieve them later.

Conclusion:

By following these steps, you should be able to recover access to your job application account. If all else fails, reaching out to customer support is the best way to get further assistance.

ITEM 5 (B).

Introduction:

If you're unable to recover your account after forgetting your password and you're having difficulty with the standard recovery steps, here are some alternative solutions you can try:

1. Contact Customer Support or Help Desk

- If you're unable to reset your password through the standard process, most job application platforms have **customer support** or a **help desk**. Reach out to them for assistance.
- Provide them with the details of your issue, such as your **email address**, **username**, and any other information that can help verify your identity.
- Many platforms have dedicated support teams that can manually verify your account and assist you in regaining access.

2. Provide Identity Verification (if Required)

- Some platforms may ask for additional **identity verification** before granting access to your account. This could include:
 - **A copy of your ID** (driver's license, passport, etc.)
 - **Answers to security questions** (if you set them up when creating the account)
 - **Proof of account ownership** (such as application history or details about previous logins)

If you have any such information, be prepared to provide it to support staff to help them verify your identity and recover your account.

3. Check for a "Contact Us" Form

- Look for a **"Contact Us"** form or a support email address on the job application site. Some sites allow you to send a direct inquiry about account issues, including password recovery.
- If you don't have access to your email and cannot reset your password, request help through the platform's official communication channels.

4. Create a New Account

- If recovery options fail and the job application platform does not allow recovery, you may need to **create a new account**.
- **Update your email address:** When creating the new account, use an **email address** that you have access to and can easily remember in the future.
- If possible, **notify the hiring company or recruiter** (if you're applying for specific jobs) that you've created a new account due to login issues.

5. Use Social Media or Forums (If Applicable)

- Some job application platforms may have an active **social media presence** (e.g., Twitter, Facebook, LinkedIn). You could reach out to them via these channels if you're not getting a response via traditional customer support.
- There may also be **user forums** or **communities** where you can ask for advice on account recovery if others have had similar issues.

6. Backup or Alternative Login Options

- Check if the platform offers **alternative login methods** (such as using **Google** or **LinkedIn** to sign in).
- If you've linked your job application account to a third-party service (e.g., Google or Facebook), try using that as a backup login method.

7. Prevent Future Issues

- Once you regain access to your account (or create a new one), consider setting up **two-factor authentication (2FA)**, if the platform supports it. This can add an extra layer of security to prevent future login issues.
- **Store your passwords securely** using a password manager, which helps you remember and manage your passwords safely.

Summary of Steps:

1. **Contact Support:** Explain your situation and ask for manual assistance.
2. **Verify Identity:** Be ready to provide verification if requested.
3. **Create a New Account:** As a last resort, create a new account with a fresh email.
4. **Alternative Login Methods:** If available, try logging in with other services (e.g., Google or LinkedIn).

Conclusion:

These steps should help you regain access to your account or find an alternative solution for applying to jobs.

ITEM 5 (C).

Introduction:

*To avoid future disruptions due to forgotten passwords for your online job application accounts, here are some practical steps you can take to **manage and secure** your passwords effectively:*

1. Use a Password Manager

A **password manager** is a tool that securely stores and organizes all your passwords. It can automatically fill in login details for websites, so you don't have to remember them all. Here's how to use one effectively:

- **Store all passwords:** Save all your job application accounts and other important credentials in one secure, encrypted place.
- **Generate strong passwords:** Most password managers can generate strong, unique passwords for each site.
- **Sync across devices:** Many password managers allow syncing across multiple devices (laptop, phone, etc.), ensuring you can access your passwords wherever you are.

Popular password managers include:

- **LastPass**
- **1Password**
- **Bitwarden**
- **Dashlane**

2. Enable Two-Factor Authentication (2FA)

Enabling **two-factor authentication (2FA)** adds an extra layer of security to your job application account. Even if you forget your password or someone tries to hack into your account, 2FA requires a second form of verification (usually a code sent to your phone or email).

- **Set up 2FA** on your job application accounts (if supported).
- **Use an authenticator app** like Google Authenticator or Authy for easy access to verification codes.

3. Create Strong, Memorable Passwords

If you prefer not to use a password manager, focus on creating strong but memorable passwords:

- **Use passphrases:** Create a password using a phrase or sentence that only you would understand. For example, "MyJobIsAwesome2025!" is both secure and easier to remember.
- **Avoid common patterns:** Don't use easy-to-guess passwords (like "password123") or personal information (like your name or birthday).
- **Use a mix of characters:** Include uppercase letters, lowercase letters, numbers, and special characters to make your password stronger.

4. Regularly Update Your Passwords

Periodically changing your password can help maintain security, especially if you haven't been using a password manager.

- Set a reminder to update your password every 3-6 months.
- Use a unique password for each site to avoid putting all your accounts at risk if one is compromised.

5. Write Down Passwords Securely (Last Resort)

If you absolutely need to write down your password, store it in a **secure place**:

- Use a **password journal** or a locked box to keep your written passwords safe.
- Avoid storing them digitally in unsecured documents (like text files or spreadsheets).

6. Set Password Recovery Options

Ensure that the **password recovery** options for your job application accounts are up to date:

- **Update your recovery email** and phone number: Make sure they're correct and accessible in case you need to reset your password.
- **Answer security questions**: If your platform supports security questions for account recovery, choose questions and answers that are easy for you to remember but hard for others to guess.
- **Link to third-party services**: If the platform allows, link your account to third-party login options like **Google** or **LinkedIn**, making it easier to access your account if you forget your password.

7. Be Cautious About Phishing

- **Don't click on suspicious links**: Be cautious of phishing attempts that ask for your login details. Always ensure that the website you're entering your credentials on is legitimate and secure (look for "https" in the URL).
- **Verify emails and messages**: If you receive emails or messages requesting you to reset your password, verify their authenticity by checking the sender's email address and not clicking any links before double-checking the platform's official site.

8. Create a Backup Email for Password Recovery

- Consider setting up a **secondary email** for password recovery purposes. This could be helpful if you lose access to your primary email or it gets compromised.
- Make sure this backup email account is secure (use a strong password and enable 2FA).

9. Sync Your Credentials Across Devices

- If you're using a **password manager**, you can sync your account credentials across devices (smartphone, tablet, laptop) to ensure you always have access to your passwords, even if you lose one device.

10. Keep Backup Copies of Important Job Information

- In case you forget your login credentials, keep a backup of your **application details** in a secure location. This could include:
 - Screenshots or saved copies of application confirmation emails.
 - A note of the positions applied for and related deadlines.

Conclusion:

By following these tips, you'll be able to significantly reduce the risk of forgetting your password and ensure smoother access to your job application accounts. Using a combination of strong password practices, 2FA, and a password manager will help safeguard your credentials and keep your job search process hassle-free!

THE END