Virtual Work Experience – Cybersecurity System Administrator

📌 **Overview**

This virtual work experience is designed to give students real-world insight into the role of a Trainee *Cybersecurity System Administrator*. As part of this experience, students will go through a structured **recruitment process**, similar to what happens in a real business.

By participating in this process, students will:

✅ Understand how businesses recruit and select candidates.

✅ Gain experience in IT system security, application management, and endpoint protection.

✅ Learn how to manage user permissions, apply security updates, and enforce patch management policies.

💼 **Application Submission**

📩 What to Submit:

- A **personal statement** (Why do you want to be a Trainee Cybersecurity System Administrator?).
- Any **relevant skills or experiences** (e.g., IT troubleshooting, operating systems, security awareness, application management).

📌 **Business Insight**: In a real workplace, employers receive applications and select candidates based on their **skills, motivation, and suitability** for the role.

🔷 Shortlisting Process:

- All applications are reviewed fairly.
- Shortlisted students move to the interview stage.

🎤 **Virtual Interview**

📅 Format: A **30-40 minute** online interview.

🎤 Who Will Interview You? A mentor from CyberSafeSchools Academy.

Interview Structure:

1) Introduction & Motivation
- Why are you interested in the Trainee Cybersecurity System Administrator role?
- What do you know about CyberSafeSchools Academy?
- Have you ever worked on IT systems, application management, or security projects before?

2) Cyber Awareness & IT Knowledge
- Why is cybersecurity important for school IT systems?
- What do you know about user permissions, role-based access controls, and authentication policies?
- How would you ensure that critical system updates and patches are applied correctly?

3) Problem-Solving & Technical Skills
- If a user requests additional permissions for an application, how would you evaluate and approve/deny the request?
- How would you enforce strong password policies across an organization?
- What steps would you take to ensure that all software applications remain secure and up to date?

4) Future Goals & Learning
- What do you hope to gain from this experience?
- Do you see yourself working in cybersecurity, system administration, or IT support in the future?

📌 **Business Insight:** In real-world recruitment, companies assess candidates based on **technical knowledge, troubleshooting skills, and problem-solving abilities**.

🔷 Scoring Criteria:
✅ Technical Curiosity & Initiative
✅ Communication & Confidence
✅ Application Security & Update Awareness
✅ Problem-Solving & Troubleshooting Skills

Next Step: Successful candidates move to the **task-based assessment** stage.

📝 **Task-Based Assessment**
🔎 Purpose: To assess technical skills, application security awareness, and troubleshooting ability.

📌 **Business Insight:** Many companies require a task-based assessment to evaluate a candidate's skills before offering a role.

Project Task: Managing Application Security and User Permissions
Your task is to implement security best practices for managing user access and application security within an organization.

🔷 Task Requirements:
- Research and summarize best practices for user access control and permissions management.
- Develop a process for granting and revoking permissions for school applications.
- Identify key risks associated with outdated applications and propose a patch management plan.
- Create a policy outlining how software updates and patches should be enforced.

🔷 Submission Format:
📄 Technical Report (Google Docs, Word) OR 📊 Slide Presentation (Google Slides, PowerPoint)

📌 Assessment Focus:
🔎 Technical Accuracy & Research Skills
🛡️ Application Security & Access Controls
🖥️ Ability to Implement Security Policies

✅ **Final Selection & Confirmation**
📧 Successful applicants receive:
- A confirmation email welcoming them to the Virtual Work Experience.
- Their assigned mentor and project details.

📌 **Business Insight:** After assessments, businesses select the best-fit candidates based on technical ability, analytical skills, and cybersecurity knowledge.

🔷 Unsuccessful applicants:
- Receive constructive feedback.
- Encouraged to reapply in the future.

🎉 **Virtual Work Experience Structure Overview**

🔷 Induction & Training – Meet mentors, learn about CyberSafeSchools, and set goals.

🔷 Project Work – Implement user access controls, security updates, and patch management policies.

🔷 Mentor Feedback & Skills Development – Learn about cybersecurity careers and system administration.

🔷 Final Presentation – Showcase your security improvement plan and findings.

📌 **Business Insight:** A Trainee Cybersecurity System Administrator must be able to manage user permissions, enforce security policies, and ensure system resilience.

🟫 **Post-Work Experience Activities**

🔷 Offboarding Process – Understanding how IT system administrators transition out of roles.

🔷 Exit Interviews – Provide feedback on the experience and discuss future opportunities.

🔷 Reference & Certification – Receive a certificate of participation and potential reference for future roles.

🔷 Networking & Alumni Connection – Stay connected with CyberSafeSchools Academy for future opportunities.

📌 **Business Insight:** Just as onboarding is crucial, the exit process ensures a smooth transition and future career opportunities for employees.

📣 **Key Takeaways for Students**

✅ Experience a real hiring process similar to business recruitment.

✅ Develop IT system administration and cybersecurity skills.

✅ Gain hands-on experience managing user permissions and software updates.

✅ Work with a mentor and present a real-world IT security improvement plan.

✅ Understand the offboarding process and its importance in a career journey.