GREAT SCHOOL OF ENGLISH

Information Security Policy	Політика інформаційної безпеки
Introduction This Information Security Policy outlines the principles, responsibilities, and practices to protect Great School of English's information assets from unauthorized access, disclosure, alteration, and destruction.	**Вступ** Ця Політика інформаційної безпеки визначає принципи, обов'язки та методи захисту інформаційних активів Great School of English від несанкціонованого доступу, розкриття, зміни та знищення**.**
Scope This policy applies to all employees, customers, including candidates, who are registered on LanguageCert approved qualifications and other visitors who have access to the organization's information systems and data.	**Сфера застосування** Ця політика поширюється на всіх співробітників, клієнтів, включаючи кандидатів, які зареєстровані на затверджених LanguageCert кваліфікаціях, та інших відвідувачів, які мають доступ до інформаційних систем та даних організації.
Objectives - To protect the confidentiality, integrity, and availability of information. - To ensure compliance with legal, regulatory, and contractual obligations. - To manage risks associated with information security.	**Цілі** - Захищати конфіденційність, цілісність і доступність інформації. - Забезпечити дотримання правових, регуляторних та договірних зобов'язань. - Управління ризиками, пов'язаними з інформаційною безпекою.
Responsibilities - Employees of Great School of English and Customers: Must adhere to this policy, report security incidents, and protect sensitive information. - IT Department: Manages security infrastructure, monitors compliance, and provides security training. - Management: Ensures adherence to policies, conducts risk assessments, and promotes security culture.	**Обов'язки** - Співробітники Great School of English та клієнти: Повинні дотримуватися цієї політики, повідомляти про інциденти безпеки та захищати конфіденційну інформацію. - IT-відділ: Керує інфраструктурою безпеки, слідкує за дотриманням вимог та проводить тренінги з безпеки. - Керівництво: Забезпечує дотримання політики, проводить оцінку ризиків та сприяє розвитку культури безпеки.
Access Control - Implement least privilege principle: users should only have access necessary for their roles. - Use strong, unique passwords and multi-factor authentication. - Regularly review and update access permissions.	**Контроль доступу** - Впроваджуйте принцип найменших привілеїв: користувачі повинні мати доступ, необхідний для виконання своїх ролей. - Використовуйте надійні, унікальні паролі та багатофакторну автентифікацію. - Регулярно переглядайте та оновлюйте права доступу.

Data Protection - Ensure secure data storage. - Implement data classification and handling procedures. - Ensure secure disposal of obsolete data and storage media.	**Захист даних** - Забезпечте безпечне зберігання даних. - Впроваджуйте процедури класифікації та обробки даних. - Забезпечте безпечну утилізацію застарілих даних та носіїв інформації.
Incident Management - Report security incidents immediately to the IT Department. - Conduct post-incident analysis and improve security measures.	**Управління інцидентами** - Негайно повідомляйте про інциденти безпеки до IT-відділу. - Проводьте аналіз після інцидентів та вдосконалюйте заходи безпеки.
Physical Security - Restrict physical access to information systems and areas where sensitive data is stored. - Use secure facilities and monitor entry points.	**Фізична безпека** - Обмежте фізичний доступ до інформаційних систем та місць, де зберігаються конфіденційні дані. - Використовуйте захищені приміщення та контролюйте точки входу.
Network Security - Use firewalls, intrusion detection systems, and antivirus software. - Regularly update software and apply patches.	**Мережева безпека** - Використовуйте брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення. - Регулярно оновлюйте програмне забезпечення та встановлюйте патчі.
Employee Training and Awareness - Conduct regular training on information security policies and best practices. - Promote awareness of phishing, social engineering, and other threats. - Evaluate employee understanding through assessments and simulations.	**Навчання та обізнаність працівників** - Проводьте регулярні тренінги з політики та передових практик інформаційної безпеки. - Підвищуйте обізнаність про фішинг, соціальну інженерію та інші загрози. - Оцінюйте розуміння співробітників за допомогою оцінювання та симуляцій.
Compliance - Regularly audit information security practices and ensure compliance with standards and regulations. - Take corrective actions for any identified non-compliance issues.	**Відповідність вимогам** - Регулярно перевіряйте практики інформаційної безпеки та забезпечуйте відповідність стандартам і правилам. - Вживайте коригувальних заходів для усунення будь-яких виявлених невідповідностей.
Review and Revision - Review this policy annually or when significant changes occur. - Incorporate feedback and continuously improve security measures. - Ensure all employees of Great School of English are informed of updates to the policy.	**Огляд і перегляд** - Переглядайте цю політику щорічно або коли відбуваються значні зміни. - Враховуйте відгуки та постійно вдосконалюйте заходи безпеки. - Переконайтеся, що всі співробітники Great School of English поінформовані про оновлення політики.

Conclusion	**Висновок**
Adherence to this Information Security Policy is essential for safeguarding the organization’s information assets and maintaining trust with partners and customers. All members of the organization are responsible for understanding and implementing these guidelines.	Дотримання цієї Політики інформаційної безпеки має важливе значення для захисту інформаційних активів організації та підтримки довіри з партнерами та клієнтами. Всі члени організації несуть відповідальність за розуміння та виконання цих правил.