سياسة الأمن السيبراني وحماية المعلومات

قسم ضمان الجودة والتطوير المؤسسي

+1 984 382 6080
VertexUniversity.edu.eu

آخر تحديث: 1 أبريل 2025

أولًا: المقدمة

في ظل التطور المتسارع في تقنيات المعلومات والاعتماد المتزايد على النظم الإلكترونية في العملية التعليمية والإدارية، تُدرك جامعة فيرتكس أهمية الأمن السيبراني كعنصر جوهري في حماية البيانات وضمان استمرارية الأعمال وتعزيز الثقة في بيئتها الرقمية.

تهدف هذه السياسة إلى وضع إطار شامل وواضح لحماية أصول المعلومات والأنظمة التقنية في الجامعة، وضمان سرية وسلامة وتوافر المعلومات المتداولة بين كافة الأطراف ذات العلاقة. كما تهدف إلى تقليل المخاطر الناتجة عن التهديدات السيبرانية، ووضع ضوابط وإجراءات استباقية واستجابية لحماية البنية التحتية الرقمية للجامعة.

تنطبق هذه السياسة على جميع منسوبي الجامعة، بمن فيهم أعضاء هيئة التدريس، الموظفين، الطلبة، المتعاونين، والموردين الذين يستخدمون أو يمكنهم الوصول إلى الأنظمة الرقمية أو البيانات الخاصة بالجامعة.

تلتزم جامعة فيرتكس بتطبيق أفضل الممارسات العالمية في الأمن السيبراني، وفقًا للمعايير المعتمدة مثل ISO/IEC 27001، وتحديث هذه السياسة دوريًا بما يتوافق مع المستجدات التقنية والتشريعية.

ثانياً: الأهداف

تهدف سياسة الأمن السيبراني وحماية المعلومات في جامعة فيرتكس إلى وضع إطار استراتيجي شامل لضمان أمن المعلومات والبنية التحتية الرقمية، ودعم البيئة التعليمية الحديثة، وذلك من خلال:

1. **حماية سرية وسلامة وتوافر المعلومات**
ضمان أمن المعلومات الأكاديمية والإدارية، ومنع الوصول غير المصرح به، والحفاظ على تكامل البيانات الرقمية في جميع أنظمة الجامعة.
2. **تعزيز الثقة في البيئة الرقمية**
توفير بيئة إلكترونية آمنة تُمكّن الطلبة وأعضاء هيئة التدريس والإداريين من أداء مهامهم بثقة واستقرار، دون تعريض بياناتهم أو أنظمتهم للمخاطر.
3. **الحد من التهديدات والمخاطر السيبرانية**
بناء منظومة دفاعية فعّالة ضد التهديدات السيبرانية، والهجمات الإلكترونية، وسد الثغرات الأمنية المحتملة من خلال تطبيق الضوابط التقنية والإدارية.
4. **تحديد المسؤوليات والصلاحيات الأمنية**
تنظيم وتوزيع أدوار ومسؤوليات جميع الجهات المعنية بأمن المعلومات داخل الجامعة، وتحديد مستويات الوصول والصلاحيات بشكل يضمن الانضباط والشفافية.
5. **دعم استمرارية الأعمال الأكاديمية والإدارية**
حماية الأنظمة والخدمات الرقمية الحيوية لضمان استمرارية العملية التعليمية والإدارية في حال وقوع أي اختراق أو حادث سيبراني.
6. **الالتزام بالمعايير والضوابط العالمية**
مواءمة سياسة الأمن السيبراني مع المعايير الدولية مثلISO/IEC 27001 ، ومعاييرNIST ، والتشريعات الوطنية ذات الصلة بحماية البيانات وأمن الشبكات.

7. **رفع الوعي والثقافة الأمنية الرقمية**
تعزيز الوعي لدى جميع منتسبي الجامعة حول أهمية الأمن السيبراني، وتدريبهم على أفضل الممارسات للوقاية من التهديدات السيبرانية وسوء استخدام البيانات.

ثالثاً: القيادة والالتزام تجاه الأمن السيبراني

تؤكد رئاسة جامعة فيرتكس والإدارة العليا التزامها الكامل بحماية أصول المعلومات وضمان أمن البنية التحتية الرقمية، باعتبار الأمن السيبراني عنصرًا استراتيجيًا في تحقيق رؤية الجامعة ورسالتها.

ويتمثل هذا الالتزام من خلال:

1. تبنّي سياسات واستراتيجيات أمن معلومات فعالة تتماشى مع المعايير الدولية والتشريعات المحلية.
2. توفير الموارد البشرية والتقنية والمالية اللازمة لتنفيذ وتطوير إطار الأمن السيبراني.
3. تعزيز ثقافة الوعي الأمني بين جميع منتسبي الجامعة عبر برامج تدريبية وحملات توعوية دورية.
4. تمكين وحدة الأمن السيبراني من أداء مهامها باستقلالية مهنية وكفاءة مؤسسية.
5. دمج الأمن السيبراني ضمن جميع القرارات المؤسسية والتقنية، لضمان استدامة الحماية الرقمية في كافة عمليات الجامعة.
6. دعم التحسين المستمر للأنظمة والإجراءات الأمنية من خلال التقييمات الدورية والمراجعة المستندة إلى الأداء والنتائج.

رابعاً: نطاق التطبيق

تنطبق سياسة الأمن السيبراني وحماية المعلومات في جامعة فيرتكس على جميع الأفراد والجهات التي تتعامل مع الأنظمة المعلوماتية أو البيانات التابعة للجامعة، وتشمل - على سبيل المثال لا الحصر - ما يلي:

1. أعضاء هيئة التدريس (دوام كامل أو جزئي)
2. الموظفون الإداريون والفنيون
3. الطلبة المسجلون في برامج الجامعة
4. المتعاونون والزوار والمستشارون
5. الشركات والموردون ومقدمو الخدمات الخارجيون
6. أي جهة أو شخص لديه صلاحية الوصول إلى الأنظمة الرقمية أو البيانات التابعة للجامعة

وتسري هذه السياسة على جميع الأنظمة والبُنى التحتية والتطبيقات والخوادم والأجهزة والبيانات الإلكترونية، سواء كانت مستضافة داخل الجامعة أو عبر بيئة الحوسبة السحابية.

كما تُعد هذه السياسة ملزمة في جميع الحالات التي يتم فيها استخدام، أو معالجة، أو تخزين، أو نقل معلومات رقمية ذات علاقة بجامعة فيرتكس أو بمنسوبيها.

خامساً: المصطلحات والتعريفات

في سياق هذه السياسة، تُستخدم المصطلحات التالية بالمعاني الموضحة أدناه، لضمان وضوح المفاهيم وتوحيد الفهم بين جميع الجهات المعنية:

- **الأمن السيبراني**

مجموعة من العمليات والتقنيات والأدوات التي تهدف إلى حماية الأنظمة الإلكترونية والشبكات والبيانات من الهجمات الرقمية أو الوصول غير المصرح به أو التدمير أو التعديل أو التعطيل.

- **البيانات الحساسة**

أي معلومات تتعلق بالطلبة، الموظفين، الكادر الأكاديمي، أو أنشطة الجامعة، والتي يتطلب حفظها سرية كاملة، مثل المعلومات الشخصية، السجلات الأكاديمية، والبيانات المالية.

- **الأصول المعلوماتية**

تشمل جميع البيانات، الأنظمة، الأجهزة، التطبيقات، والبنية التحتية التقنية التي تُستخدم أو تُدار داخل الجامعة أو ترتبط بها.

- **الحدث السيبراني**

أي حدث يؤثر أو يُحتمل أن يؤثر سلبًا على سرية أو سلامة أو توافر نظم المعلومات، مثل الاختراقات، البرمجيات الخبيثة، التصيّد الإلكتروني، أو الأعطال التقنية المتعمدة.

- **الوصول غير المصرح به**

الوصول إلى أنظمة أو بيانات الجامعة من قبل أفراد أو جهات لا تمتلك الصلاحية أو الإذن الرسمي بذلك.

- **التشفير**

آلية لتحويل البيانات إلى صيغة غير مفهومة لحمايتها من الاطلاع أو الاستخدام من قبل أطراف غير مخوّلة، سواء أثناء التخزين أو النقل.

- **النسخ الاحتياطي**

عملية حفظ نسخة من البيانات بشكل دوري في موقع آمن لضمان استرجاعها في حال فقدانها أو تعرضها لهجوم أو خلل تقني.

- **البرامج الخبيثة**

برمجيات ضارة تهدف إلى التسلل أو التخريب أو سرقة المعلومات من الأنظمة، وتشمل الفيروسات، Ransomware، و Spywareوغيرها.

سادساً: السياسات العامة للأمن السيبراني

تلتزم جامعة فيرتكس بتطبيق مجموعة من السياسات العامة التي تُشكل الإطار الأساسي لحماية أنظمتها المعلوماتية ومصادر بياناتها، وذلك لضمان أعلى مستويات الأمان والاستمرارية. وتشمل هذه السياسات:

1.سياسة حماية سرية المعلومات

يجب حماية جميع المعلومات الحساسة والمتعلقة بالطلبة، والموظفين، والبرامج الأكاديمية من الوصول غير المصرح به أو الكشف أو الاستخدام غير المشروع، سواء كانت محفوظة داخل الجامعة أو على خدمات الحوسبة السحابية.

2.سياسة النزاهة وسلامة البيانات

يجب ضمان أن جميع البيانات محفوظة بدقة وكاملة وغير خاضعة للتعديل غير المصرح به أثناء التخزين أو النقل أو المعالجة، مع تطبيق ضوابط تحقق متعددة المستويات.

3.سياسة توافر الأنظمة والخدمات

تلتزم الجامعة بضمان استمرارية عمل الأنظمة والخدمات الرقمية دون انقطاع، من خلال خطط استجابة للطوارئ، نسخ احتياطي دوري، وبنية تحتية مرنة.

4.سياسة الوصول إلى الأنظمة

يُمنح الوصول إلى المعلومات والأنظمة فقط للمستخدمين المخوّلين حسب طبيعة مهامهم، ويتم التحكم به من خلال آليات تحقق متعددة، وإدارة دورية للصلاحيات.

5.سياسة كلمات المرور

يجب استخدام كلمات مرور قوية وفريدة لكل مستخدم، وتحديثها بشكل دوري. ويُمنع مشاركة كلمات المرور أو حفظها في أماكن غير آمنة.

6.سياسة إدارة الحوادث السيبرانية

يجب على جميع المستخدمين الإبلاغ الفوري عن أي حادث سيبراني مشتبه به، وفقًا لإجراءات الإبلاغ المعتمدة، وتقوم وحدة الأمن السيبراني بالتحقيق والاستجابة السريعة وفق بروتوكولات مدروسة.

7.سياسة الاستخدام المقبول

يُمنع استخدام أنظمة الجامعة لأغراض شخصية ضارة، أو تحميل برامج غير مرخصة، أو استخدام الموارد في أنشطة مخالفة للقوانين أو الأخلاقيات الأكاديمية.

8.سياسة التحديث والتصحيح الأمني

يجب تحديث جميع الأنظمة والبرمجيات بشكل منتظم لضمان معالجة الثغرات الأمنية، بالتنسيق مع وحدة تقنية المعلومات في الجامعة.

سابعاً: منهجية الأمن السيبراني

تعتمد جامعة فيرتكس في تنفيذ سياساتها الأمنية على منهجية متكاملة تقوم على المبادئ التالية:

1.النهج القائم على تقييم المخاطر

تُطبق الجامعة آلية منهجية لتحديد وتقييم وإدارة المخاطر السيبرانية المرتبطة بالأنظمة، والبيانات، والمستخدمين. ويتم تصنيف المخاطر حسب درجة تأثيرها، وتُعطى الأولوية للإجراءات التي تقلل من احتمالية وقوع الحوادث ذات الأثر المرتفع.

2.مبدأ الدفاع متعدد الطبقات

تُبنى أنظمة الأمن السيبراني في الجامعة على طبقات متداخلة من الحماية تشمل: التحكم في الوصول، التشفير، أنظمة كشف التسلل، الجدران النارية، النسخ الاحتياطي، وضوابط الاستخدام، لضمان مواجهة التهديدات من عدة اتجاهات.

3.أتمتة وتحديث الإجراءات الأمنية

تسعى الجامعة إلى أتمتة العمليات الأمنية الحيوية، مثل كشف التهديدات، إدارة الثغرات، وإصدار التنبيهات، لضمان استجابة أسرع وأكثر دقة، مع الحرص على تحديث البرمجيات والسياسات بشكل مستمر.

4.الاستجابة والتعافي من الحوادث

تمتلك الجامعة خطة استجابة للحوادث السيبرانية تشمل: الاكتشاف، التقييم، الاحتواء، المعالجة، والتوثيق. كما تم إعداد خطط للتعافي واستعادة الأنظمة والبيانات لضمان استمرارية العمليات التعليمية والإدارية.

5.المواءمة مع المعايير العالمية

تلتزم الجامعة بتطبيق أفضل الممارسات الأمنية المعترف بها عالميًا، بما في ذلك:

ISO/IEC 27001، **NIST Cybersecurity Framework**،

وضوابط الحوكمة الرقمية الصادرة عن الجهات الوطنية ذات العلاقة.

6.التحسين المستمر

تُراجع هذه المنهجية بشكل دوري من خلال تقييمات داخلية وخارجية، بهدف تحسين الأداء الأمني، وتكييف السياسات والإجراءات مع التغيرات في التهديدات التكنولوجية والتشريعية.

ثامناً: المسؤوليات

تُحدد سياسة الأمن السيبراني بجامعة فيرتكس المسؤوليات بوضوح لضمان تنفيذ الإجراءات الأمنية بكفاءة وفعالية على كافة المستويات الإدارية والأكاديمية. وتشمل الأدوار التالية:

1. رئاسة الجامعة والإدارة العليا:

- اعتماد سياسة الأمن السيبراني والتأكد من مواءمتها مع استراتيجية الجامعة.
- دعم تنفيذ السياسات وتوفير الموارد اللازمة لضمان فاعلية تطبيقها.

2. وحدة تقنية المعلومات والأمن السيبراني:

- تنفيذ السياسة ومراقبة الامتثال لجميع الضوابط الأمنية.
- تقييم المخاطر السيبرانية بشكل دوري وتطبيق خطط الاستجابة للحوادث.
- إدارة صلاحيات الوصول إلى الأنظمة والمعلومات.
- إجراء النسخ الاحتياطي، والتحديثات الأمنية، وإجراءات الحماية التقنية.
- تقديم الدعم الفني والتدريب في مجال الأمن السيبراني.

3. الجهات الأكاديمية والإدارية:

- الالتزام بتطبيق السياسات والإجراءات الأمنية في وحداتهم التنظيمية.
- التأكد من أن الموظفين تحت إشرافهم يستخدمون الأنظمة بطريقة آمنة ومسؤولة.

4. أعضاء هيئة التدريس والموظفون:

- الالتزام التام بكافة سياسات الأمن السيبراني المعتمدة من الجامعة.
- الإبلاغ الفوري عن أي تهديد أو حادث سيبراني لوحدة الأمن السيبراني.
- الحفاظ على سرية المعلومات وعدم مشاركتها دون تصريح رسمي.

5. الطلبة والمستخدمون الخارجيون:

- استخدام الأنظمة الإلكترونية والموارد الجامعية بطريقة مسؤولة وآمنة.
- الامتناع عن أي محاولة لاختراق أو التلاعب بالأنظمة أو الوصول غير المصرح به.
- الالتزام بالتعليمات الخاصة بكلمات المرور واستخدام البريد الإلكتروني الجامعي.

تاسعاً: ضوابط الوصول وإدارة الصلاحيات

تلتزم جامعة فيرتكس بتطبيق نظام دقيق لإدارة الوصول إلى الأصول الرقمية والمعلوماتية، لضمان استخدام الأنظمة والبيانات فقط من قبل الأشخاص المخوّلين، وفقًا لصلاحياتهم الوظيفية.

وتشمل ضوابط الوصول المعتمدة ما يلي:

1. مبدأ الحد الأدنى من الصلاحيات

يتم منح كل مستخدم صلاحيات محدودة ومتناسبة مع طبيعة عمله ومسؤولياته، ويُمنع منح صلاحيات غير ضرورية.

2.التحقق متعدد العوامل

تُستخدم آليات تحقق مزدوجة أو متعددة للوصول إلى الأنظمة الحساسة، مثل تسجيل الدخول عبر كلمة مرور ورمز تحقق مرسل للجوال أو البريد الإلكتروني.

3.إدارة الحسابات والصلاحيات

- يتم إنشاء الحسابات الرسمية من خلال وحدة تقنية المعلومات فقط.
- تُراجع الصلاحيات بشكل دوري لضمان توافقها مع تغييرات المهام أو التعيينات.
- تُلغى صلاحيات المستخدم فور انتهاء العلاقة الرسمية مع الجامعة (مثل الاستقالة أو التخرج).

4.تسجيل ومراقبة محاولات الدخول

يتم تسجيل جميع محاولات الدخول إلى الأنظمة، ومراقبتها للكشف عن أي نشاط غير معتاد أو محاولات اختراق.

5.ضوابط الوصول إلى البيانات الحساسة

يُمنح الوصول إلى البيانات الحساسة فقط للجهات المخوّلة رسميًا، ويُشترط وجود موافقات واضحة وآليات مراجعة دورية.

6.الوصول الخارجي وخدمات السحابة

يُنظم الوصول إلى أنظمة الجامعة من خارج الحرم الرقمي، ويخضع لضوابط أمنية مشددة، بما في ذلكVPN ، والتشفير، وتحديد العناوين المسموح بها.

7.استخدام الأجهزة الشخصية

عند السماح باستخدام أجهزة شخصية للوصول إلى أنظمة الجامعة، تُطبق سياسات صارمة مثل تشفير البيانات، واستخدام برامج الحماية، وربط الأجهزة بالمصادقة المؤسسية.

عاشراً: إدارة الحوادث السيبرانية

تولي جامعة فيرتكس أهمية قصوى للاستجابة السريعة والفعّالة لأي حادث سيبراني قد يؤثر على سرية أو سلامة أو توافر أنظمتها ومعلوماتها الرقمية، بما يضمن الحد من الأضرار واستمرارية الأعمال.

وتشمل آلية إدارة الحوادث السيبرانية في الجامعة ما يلي:

1.تعريف الحادث السيبراني:

يُقصد به أي محاولة ناجحة أو فاشلة لاختراق أو تعطيل أو استغلال أو الوصول غير المصرح به إلى الأنظمة أو الشبكات أو البيانات التابعة للجامعة، بما في ذلك:

- الهجمات الخبيثة(Malware, Ransomware)
- التصيّد الإلكتروني(Phishing)
- تسريب أو فقدان البيانات

- أعطال الأنظمة نتيجة أعمال عدائية أو إهمال

2.إبلاغ الحوادث

- يجب على جميع منتسبي الجامعة الإبلاغ الفوري عن أي حادث أو نشاط مشبوه إلى وحدة الأمن السيبراني عبر القنوات المعتمدة.
- يتم توفير نموذج موحّد للإبلاغ، ويُتاح إلكترونيًا عبر نظام الدعم الداخلي للجامعة.

3.التحقق والتصنيف:

- تتولى وحدة الأمن السيبراني فحص البلاغات وتقييم مستوى الخطر (منخفض، متوسط، عالٍ)
- تُصنّف الحوادث حسب طبيعتها وتأثيرها على الأنظمة والبيانات.

4.الاستجابة واحتواء الحادث:

- يتم تنفيذ خطة استجابة فورية تشمل احتواء الحادث، عزل الأنظمة المتأثرة، وتطبيق إجراءات استباقية لوقف الضرر.
- تُنسّق الجهود بين وحدة الأمن السيبراني ووحدات تقنية المعلومات والإدارات المعنية.

5.التحقيق والتحليل:

- تُجري الوحدة المختصة تحقيقًا شاملًا لتحديد مصدر الحادث، أساليبه، الثغرات المستغلة، ومدى تأثيره.
- تُوثّق نتائج التحقيق وتُستخدم لتحسين السياسات والإجراءات.

6.التعافي واستعادة الأنظمة

- تُفعل خطط النسخ الاحتياطي لاستعادة الأنظمة والبيانات المتضررة.
- يتم اختبار الأنظمة المتعافية والتأكد من سلامتها قبل إعادتها إلى بيئة التشغيل.

7.التوثيق والتقرير النهائي:

- يتم إعداد تقرير نهائي مفصل لكل حادث، يشمل التوصيات والإجراءات التصحيحية.
- يُحتفظ بالتقارير ضمن سجل الحوادث السيبرانية المعتمد داخل الجامعة.

8.المراجعة والتعلم من الحوادث:

- يتم تحليل الأنماط المتكررة واستخلاص الدروس المستفادة لتحسين قدرة الجامعة على الاستجابة المستقبلية.
- تُحدث الضوابط الأمنية والإجراءات الفنية بناءً على نتائج التحقيق.

الحادي عاشر: التوعية والتدريب السيبراني

تؤمن جامعة فيرتكس أن بناء ثقافة أمنية قوية بين جميع منتسبيها يُشكل خط الدفاع الأول ضد التهديدات السيبرانية. وبما أن الجامعة تعمل بالكامل في بيئة إلكترونية، فإن التوعية والتدريب السيبراني يشكلان جزءًا أساسيًا من استراتيجية الحماية الرقمية.

ولذلك، تلتزم الجامعة بما يلي:

1.برامج توعوية دورية:

تنظم الجامعة حملات توعوية رقمية تستهدف جميع الفئات (الطلبة، الموظفين، أعضاء هيئة التدريس) لتوضيح مخاطر الأمن السيبراني وأفضل الممارسات للوقاية.

2.دورات تدريب إلكترونية:

توفر الجامعة برامج تدريبية إلكترونية متخصصة في موضوعات مثل:

- إدارة كلمات المرور
- التعرّف على رسائل التصيّد
- حماية الأجهزة الشخصية
- أمن البريد الإلكتروني
- سياسة الاستخدام المقبول

3.إلزامية التدريب للموظفين الجدد:

يشترط اجتياز دورة تمهيدية في الأمن السيبراني لجميع الموظفين الجدد قبل منحهم صلاحية الوصول إلى الأنظمة الحساسة.

4.تقييم الوعي الأمني:

تُجري وحدة الأمن السيبراني اختبارات دورية وقياسات لمستوى الوعي بين المستخدمين، ويتم استخدام النتائج لتحديد الثغرات التدريبية.

5.نشرات وتنبيهات أمنية:

تُنشر تنبيهات دورية حول التهديدات السيبرانية الجديدة، وإرشادات التعامل معها، عبر البريد الإلكتروني الرسمي أو لوحة الإعلانات الرقمية للجامعة.

الثاني عاشر: مراجعة السياسة وتحديثها

تُراجع سياسة الأمن السيبراني وحماية المعلومات في جامعة فيرتكس بشكل دوري لضمان توافقها مع:

- التطورات التقنية المستجدة
- التهديدات السيبرانية الحديثة
- المتطلبات القانونية والتنظيمية
- معايير الجودة والاعتماد المؤسسي

وتكون مسؤولية المراجعة على عاتق وحدة الأمن السيبراني بالتعاون مع الإدارة العليا ووحدة تقنية المعلومات، ويتم:

- تحديث السياسة مرة واحدة على الأقل سنويًا، أو عند حدوث تغيير جوهري في البنية الرقمية أو التشريعات المعتمدة.
- توثيق جميع التعديلات المعتمدة، وتوزيع النسخة المحدثة على الجهات المعنية داخل الجامعة.

- نشر النسخة الأحدث من السياسة على الموقع الداخلي الرسمي للجامعة.

الثالث عاشر: المخالفات والعقوبات

تُعد سياسة الأمن السيبراني وحماية المعلومات وثيقة ملزمة لجميع مستخدمي أنظمة جامعة فيرتكس الرقمية، ويُعد أي خرق لهذه السياسة - سواء كان متعمدًا أو ناتجًا عن إهمال - تصرفًا يُعرّض صاحبه للمساءلة وفقًا للأنظمة المعتمدة داخل الجامعة.

وتُصنّف المخالفات إلى:

1.المخالفات البسيطة:

مثل مشاركة كلمات المرور، أو استخدام البريد الإلكتروني لأغراض غير مصرح بها، أو الدخول إلى بيانات غير حساسة بدون إذن.

العقوبات المحتملة:
تنبيه رسمي - تدريب إلزامي - تعليق مؤقت للصلاحيات

2.المخالفات المتوسطة:

مثل تثبيت برامج غير مرخصة، أو تخزين معلومات حساسة بدون حماية كافية، أو تجاهل تحديثات الأمان.

العقوبات المحتملة:
إنذار رسمي - سحب الصلاحيات مؤقتًا - جلسة تحقيق داخلية - إلزام بإجراءات تصحيحية

3.المخالفات الجسيمة:

مثل محاولة اختراق أنظمة الجامعة، تسريب أو إتلاف بيانات حساسة، استخدام الأنظمة لأغراض عدائية، أو التواطؤ في أنشطة سيبرانية ضارة.

العقوبات المحتملة:
إنهاء الخدمة - فصل الطالب - إحالة إلى الجهات القانونية أو التأديبية - تعويض الأضرار

الرابع عاشر: الإتصال

للاستفسارات المتعلقة بسياسة الأمن السيبراني وحماية المعلومات، يرجى التواصل معنا عبر:

جامعة Vertex
Email: info@vertexuniversity.edu.eu
Address: Vertex University, California, USA