جامعة الأمير سطام بن عبد العزيز

وثائق نظام إدارة أمن المعلومات

سياسة التعامل مع حوادث أمن المعلومات

في

عمادة تقنية المعلومات والتعليم عن بعد

جدول المحتويات

1. تفاصيل الوثيقة

1.1 البيانات الأساسية

المؤسسة	جامعة الأمير سطام بن عبد العزيز عمادة تقنية المعلومات والتعليم عن بعد
العنوان	سياسة التعامل مع حوادث أمن المعلومات
جهة الإصدار	فريق نظام إدارة أمن المعلومات
تاريخ الإصدار	25 يونيو 2015
التصنيف الأمني	○ عام ⊙ داخلي ○ محظور ○ سري
رقم النسخة	الإصدار رقم 1
عدد الصفحات	13

1.2 تحرير الوثيقة

النسخة	الاسم/ الإدارة	نوع النسخة	راجعها/ اعتمدها	التاريخ	ملاحظات
0.1	مأمون السعيد (مستشار أمن معلومات)	مسوّدة		25 يونيو 2015	

2. التحكّم بالإصدارات

2.1 الموافقة على التغييرات

لا يجوز الاطلاع على هذه الوثيقة، أو طباعتها أو توزيعها إلا من قبل الموظفين المفوضين فقط. وينبغي مراجعة أية تغييرات عليها واعتمادها من قبل مدير نظام إدارة أمن المعلومات.

2.2 التوزيع

لا يجوز الاطلاع على هذه الوثيقة، أو طباعتها أو توزيعها إلا من قبل الموظفين المفوضين فقط. يجب العمل باستمرار على إدراج الجهات التي تحصل على نسخة من هذه الوثيقة ضمن الجدول المبين أدناه.

رقم النسخة	المستلم/ الإدارة	التوقيع
.1	عميد تقنية المعلومات والتعليم عن بعد	
.2	مدير أدارة المشاريع	
.3	رئيس قسم التطبيقات وقواعد البيانات	
.4	مدير قسم مركز البيانات	
.5	قسم أنظمة التشغيل والشبكات	
.6	قسم خدمات تقنية المعلومات والدعم	
.7	قسم أمن تقنية المعلومات	

3. الأهداف

تهدف هذه السياسة إلى وضع إطار للتعامل مع حوادث حماية المعلومات بفعالية ودون تأخير. وتعرّف حادثة أمن المعلومات بأنها انتهاك يشك في حدوثه أو أن حدوثه مؤكد لدقة وتوافر وسرية معلومات، بما يتسبب أو يكون قد تسبب بالتأثير على أمن معلومات عمادة تقنية المعلومات والتعليم عن بعد في جامعة الأمير سطام بن عبد العزيز.

فيما يلي أهداف مشروع إدارة نظام إدارة أمن المعلومات ومجهودات أمن المعلومات التي تقوم بها عمادة تقنية المعلومات والتعليم عن بعد.

- إرساء قواعد المسؤولية والمساءلة عن أمن المعلومات في العمادة.
- التأكّد من أن لدى موظفي عمادة تقنية المعلومات والتعليم عن بعد توعية سليمة واهتماماً بأمن أنظمة المعلومات؛ وتقدير كافٍ لمسؤولياتهم على صعيد أمن المعلومات.
- التأكّد من قدرة عمادة تقنية المعلومات والتعليم عن بعد على التعامل مع مخاطر أمن المعلومات وخفضها.
- التأكّد من قدرة عمادة تقنية المعلومات والتعليم عن بعد على مواصلة تقديم خدماتها الحيوية بأسلوب يتسم بالاحترافية والتنظيم ومراعاة الجوانب الأمنيّة.
- التأكّد من مواصلة امتثال عمادة تقنية المعلومات والتعليم عن بعد للقوانين واللوائح، والسياسات الداخلية بما في ذلك معيار الأيزو 27001:2013.
- التأكّد من تطبيق آليات التحكّم المطلوبة لحماية سرية وتكامل وتوافر الأصول المعلومات لعمادة تقنية المعلومات والتعليم عن بعد.

4. النطاق

تنطبق هذه السياسة على جميع عمليات ومهام تقنية المعلومات بعمادة تقنية المعلومات والتعليم عن بعد، وعلى جميع مستخدمي الأصول المعلوماتية بما في ذلك الموظفين الموقّتين والدائمين في العمادة، وأعضاء هيئة التدريس، والعملاء، والاستشاريين، والموردين، وشركاء العمل والموظفين التابعين للمقاولين؛ بغض النظر عن الموقع الجغرافي.

تشمل هذه السياسة على جميع الأنظمة والأصول المعلومات لتقنية المعلومات بعمادة تقنية المعلومات والتعليم عن بعد، سواء أكانت تُدار من قبل العمادة أو من قبل طرف ثالث، بما في ذلك، على سبيل المثال لا الحصر:

- أجهزة الخادم، ومحطات العمل وجميع معدات البنية التحتية للحاس الآلي.
- البنية التحتية للشبكة ومعداتها.
- برمجيات وتطبيقات تقنية المعلومات.
- المعلومات أو البيانات الإلكترونية المخزّنة في الملفات وقواعد البيانات والوثائق الورقية.
- جميع موظفي ومستخدمي تقنية المعلومات.

5. الاستثناءات

قد تنشأ حالات استثنائية أو طارئة تحول دون تطبيق جزء أو أجزاء من هذه السياسة. وفي مثل هذه الحالة، ينبغي تقديم طلب استثناء رسمي مشفوعاً بالمبررات، إلى مدير نظام إدارة أمن المعلومات، والذي يبادر بتقييم الطلب، والبحث في البدائل المجدية، واتخاذ القرار الملائم.

6. إنفاذ السياسة والانتهاكات

يتعين على جميع الإدارات بعمادة تقنية المعلومات والتعليم عن بعد والموظفين والمقاولين والموردين والشركاء، الالتزام الثابت والمتواصل بقواعد وسياسات هذه السياسة.

وعلى رؤساء أقسام تقنية المعلومات بالعمادة تقنية المعلومات والتعليم عن بعد التأكّد من المراقبة الدائمة للالتزام به ضمن الأقسام التي تقع تحت مسؤوليتهم. يخضع الالتزام بالقواعد الواردة في هذه السياسة للمراجعة الدورية من قبل مدير نظام إدارة أمن المعلومات، ومن شأن عدم الالتزام بالإطار العام له أن يُسفر عن القيام بإجراءات تصحيحية قد تشمل تطبيق إجراءات انضباطية، على أن تكون هذه الإجراءات متوافقة مع درجة المخالفة، وقد تشمل على سبيل المثال لا الحصر:

- توجيه إنذار شفوي.
- إنهاء العقد.
- اتخاذ إجراءات قانونية.

7. مُلكية الوثيقة

يتولى مدير نظام إدارة أمن المعلومات مُلكيّة هذه الوثيقة، وينبغي الحصول على موافقته الصريحة على أية تغييرات أو تحديثات على هذه الوثيقة.

8. الأدوار ومجالات المسئولية

الدور	مجال المسئوليات
مسئول أمن المعلومات	• وضع وتحديد إجراءات مناسبة لتداول، ومعالجة، وتخزين وتعميم المعلومات. • تحديد الأدوار والمسئوليات الأمنيّة لكل اتفاقية من اتفاقيات مستوى الخدمة. • التدقيق على دخول الطرف الثالث من حيث الانتهاكات الأمنية، أو إساءة الاستخدام وتقييم الاحتياجات.
عمادة تقنية المعلومات	• المراقبة الأمنية للنظام/ التطبيق/ الشبكة. • تركيب البنية التحتية الحيوية لأمن المعلومات (مثل البنية التحتية لبرامج مكافحة الفيروس) • تصميم وتطبيق أمن الشبكة والنظام. • تطبيق ضوابط ملائمة لحماية سرية ودقة وصحة المعلومات الحساسة. • تنسيق الاستجابة للانتهاك الفعلية، أو التي يُشك بحدوثها، لسرية، أو دقة، أو توافر نظم المعلومات الحيوية. • التحقيق في انتهاكات الضوابط، وتطبيق ضوابط تعويضية إضافية عند الضرورة. • تطبيق ضوابط ملائمة لحماية وضبط معلومات نظم الأتمتة. • تطبيق التغييرات وتركب برامج إصلاح النظم (Patching) على النظم/ التطبيقات/ الشبكة وفقا لإجراءات إدارة التغيير وإجراءات إدارة برامج إصلاح النظم (Patch)
وحدة المشروع	• المشاركة في تحديد الأدوار والمسئوليات الأمنية المطلوبة لاتفاقيات مستوى الخد واتفاقيات تبادل المعلومات. • إدارة العلاقة مع الطرف الثالث.
مالك الأصل	• تحديد حقوق دخول مستخدمي المعلومات إلى الأصول المعلوماتية الموجودة على نظم المعلومات.
المستخدم / الموظف	• الالتزام بسياسات، وإرشادات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات. • إبلاغ عمادة تقنية المعلومات بالحوادث الأمنية الفعلية أو تلك التي تثير الشكوك.

9. الإطار العام للسياسة

9.1 الإبلاغ عن حوادث أمن المعلومات

- يجب أن يكون لدى أعضاء هيئة التدريس، والموظفين، والطلاب والمقاولين والاستشاريين القدرة على إدراك، وإمكانية التعرّف على السلوكيات غير المتوقعة أو غير الاعتيادية للأصول، والتي قد تمثل خللا محتملا في البرمجيات. وتتضمن الأحداث الأمنية ما يلي، وذلك على سبيل المثال لا الحصر:
  أ. تغييرات على النظام لا تكون تحت السيطرة.
  ب. انتهاك قواعد الدخول (مثل المشاركة في كلمة المرور).
  ج. انتهاك الأمن المادي.
  د. اختراق النظام أو السيطرة عليه.
- في حالة اكتشاف حدث أمني، يتوجب على المستخدمين القيام بما يلي:
  أ. ملاحظة الأعراض وأية رسائل أخطاء على الشاشة.
  ب. فصل محطة العمل عن الشبكة فيما لو كانت هناك أية شكوك بتأثر أي من الأجهزة (بمساعدة عمادة تقنية المعلومات).
  ج. عدم استخدام أية وسائط قابلة للنقل (على سبيل المثال ذاكرة الفلاش) قد تكون تأثرت أيضا.
- على جميع أعضاء هيئة التدريس، والموظفين، والطلاب والمقاولين والاستشاريين في الجامعة إبلاغ عمادة تقنية المعلومات على الفور بأي حدث أمني. على أن يتم توفير المعلومات التالية، وذلك على سبيل المثال لا الحصر:
  أ. اسم جهة الاتصال ورقم الشخص الذي أبلغ عن الحادثة.
  ب. نوع المعلومات أو الأجهزة المتأثرة.
  ج. بيان فيما إذا كان فقدان المعلومات قد يعرض أي شخص أو بيانات للخطر.
  د. موقع الحادثة.
  هـ. أرقام الجرد الخاصة بأي جهاز متأثر بالحادثة.
  و. تاريخ ووقت وقوع الحادثة.
  ز. موقع البيانات أو الأجهزة المتأثرة.
  ح. نوع وظروف الحادثة.
- يتعين على عمادة تقنية المعلومات تطبيق إجراءات رسمية "إجراءات الاستجابة لحوادث أمن المعلومات" يتم من خلالها تحديد الخطوات اللازمة للتعامل مع أي حادثة تتعلق بأمن المعلومات.

9.2 الإبلاغ عن نقاط الضعف الأمنية

- يتعيّن على جميع أعضاء هيئة التدريس، والموظفين، والطلاب والمقاولين والاستشاريين في الجامعة الإبلاغ عن أية ثغرات تتصل بأمن المعلومات يشك في وجودها في النظم أو الخدمات.
- يتعين العمل، وبأسرع وقت ممكن، على إبلاغ عمادة تقنية المعلومات والتعليم عن بعد بخصوص أية ثغرات في أمن المعلومات، واتباع إجراءات الاستجابة للحادثة والتصعيد. وقد تتضمن الثغرات الأمنية ما يلي، وذلك على سبيل المثال لا الحصر:
  أ. حماية غير كافية من قبل الجدار الناري أو برنامج الحماية من الفيروسات.
  ب. خلل في عمل النظام أو زيادة الحمولة.
  ج. خلل في عمل برامج التطبيقات.
  د. أخطاء بشرية.

9.3 المسئوليات والإجراءات

- يجب العمل على بيان مسئوليات عمادة تقنية المعلومات ووضع إجراءات ملائمة لضمان فعالية الاستجابة لأحداث أمن المعلومات.
- على جميع أعضاء هيئة التدريس، والموظفين، والطلاب والمقاولين والاستشاريين في الجامعة تفهّم مسئولياتهم المتعلقة بالإبلاغ عن الحوادث الأمنية.
- يتعين على مسئول أمن المعلومات وعمادة تقنية المعلومات تطوير إجراءات لإدارة الحوادث الأمنية، بحيث تتضمن هذه الإجراءات ما يلي، وذلك على سبيل المثال لا الحصر:
  أ. التعرف على الحادثة، وتحليلها للتأكد من سببها ونقاط الضعف الأمنية التي جرى استغلالها.
  ب. الحد من أو تقليص أية أثار أخرى للحادثة.
  ج. أساليب احتواء الحادثة.
  د. الإجراءات التصحيحية الرامية إلى معالجة الحادثة والحيلولة دون تكرارها.
  هـ. إبلاغ كافة المتأثرين على امتداد الجامعة.
  و. جمع أية أدلة.
- يتعين تصنيف كافة المعلومات ذات الصلة بالحادثة الأمنية بناء على مخطط التصنيف الحالي للحوادث الأمنية. وتتولى عمادة تقنية المعلومات والتعليم عن بعد مسئولية تخصيص مستوى التصنيف الملائم لكل حادثة أمنية بعد الحصول على إدارة العمادة.
- تخضع إجراءات التعافي من الحادثة لضوابط رسمية. وينبغي عدم تمكين أية جهة، باستثناء الموظفين المفوضين، من الوصول إلى نظام المعلومات المتأثر خلال الحادثة، وأن يتم توثيق كافة التدابير العلاجية مع توفير أكبر قدر من التفاصيل بخصوصها.
- يتعين على عمادة تقنية المعلومات والتعليم عن بعد وضع "نموذج إدارة حوادث أمن المعلومات" بهدف الإبلاغ عن كافة الانتهاكات/ الحوادث الأمنية مما يؤسس لآلية استجابة سريعة لحوادث أمن المعلومات.
- يتعين على عمادة تقنية المعلومات والتعليم عن بعد نشر، أينما أمكن، نظام للمراقبة لاكتشاف حوادث أمن المعلومات.
- يحظر الإفصاح عن المعلومات ذات الصلة بحوادث أمن المعلومات على أي طرف ثالث (الجمهور، الصحافيين، وغيرهم).
- يجب تحليل كافة حوادث أمن المعلومات التي تؤدي إلى تعطل الخدمة أو خسارة في الأصول، وذلك بهدف التحقق من وجود اتجاهات معيّنة للحوادث. وينبغي إبلاغ مسئول أمن المعلومات وعمادة تقنية المعلومات عن مثل هذه الحوادث ووضعهم بصورة تحليل الاتجاهات بصورة دورية.

- على عمادة تقنية المعلومات والتعليم عن بعد تقييم حادثة أمن المعلومات من حيث أهميتها، بناء على الآثار التي لحقت أو يمكن أن تلحق بالعمل.
- ينبغي لإجراء الاستجابة للحادثة أن يمثل استمراريةَ تتسم بالسلاسة لإجراءات الإبلاغ عن الحادثة الأمنية، وأن يتضمن خططا للطوارئ لضمان استمرارية نظم المعلومات خلال الحادثة.
- يجب إبلاغ الموظفين ذوي العلاقة، بأية حوادث أمن معلومات محتملة، وينبغي عليهم المساعدة في الإجراءات العلاجية التي سيتم اتخاذها.
- تتولى عمادة تقنية المعلومات مسئولية متابعة وضع الحادثة والمتابعة مع الأشخاص ذوي العلاقة والتعامل مع الاستفسارات المتعلقة بالتطورات على الحادثة. ويتعين تسجيل كافة حوادث أمن المعلومات، وتخصيص رقم لها، ليمكن من خلاله تعقبها والرجوع إليها مستقبلا. ويتضمن سجل الحوادث الأمنية ما يلي، وذلك على سبيل المثال لا الحصر:
  أ. **الأسباب:** سواء أسهمت بصورة مباشرة أو غير مباشرة في وقوع الحادثة.
  ب. **الآثار:** ما هي نظم المعلومات التي تأثر بوقوع الحادثة الأمنية؟
  ج. **الإجراء الذي تم اتخاذه:** من قبل المستخدم وعمادة تقنية المعلومات من حيث الإبلاغ عن الحادثة وإدارتها.
  د. **مستوى الضرر:** ما هي الخسائر التي نجمت؟
  هـ. **تاريخ ووقت وقوع الحادثة.**

9.4 الاستفادة من حوادث أمن المعلومات

- تقوم عمادة تقنية المعلومات بمقارنة المعلومات التي توفرت بعد الحادثة ومراجعتها بصورة منتظمة. كما يجب العمل رسميا على تدوين أية تغييرات تمت على الإجراءات نتيجة لمراجعة ما بعد الحادثة.
- في أعقاب وقوع أية حادثة، يتعيّن أن تقوم عمادة تقنية المعلومات والتعليم عن بعد بإجراء تمرين حول الدروس المستفادة، وتوثيق النتائج بصورة كافية.

9.5 جمع الأدلة

- يتولى مسئول أمن المعلومات وعمادة تقنية المعلومات والتعليم عن بعد تحديد، وتوثيق، وإدامة قواعد جمع الأدلة، والاحتفاظ بها، وتقديمها بناء على المتطلبات الأمنية والتنظيمية والقانونية للجامعة.
- فيما لو تطلبت إحدى الحوادث الأمنية الحصول على بعض المعلومات لتسهيل سير التحقيق، فيجب الالتزام بالقواعد بدقة بالغة. ويتوجب التعامل بحذر مع عملية جمع الأدلة للتحقيقات المحتملة.
- يتعين الاتصال بمسئول أمن المعلومات وعمادة تقنية المعلومات على الفور بخصوص أية إرشادات، والالتزام بالإجراءات بدقة عندما يتعلق الأمر بجمع الأدلة الجنائية.

10. الملاحق

10.1 المصطلحات والاختصارات

المصطلح	Term	التعريف
مساءلة	**Accountability**	مبدأ أمني يدل على وجوب تحديد الأشخاص وتحميلهم مسؤولية تصرفاتهم.
حقوق/ امتيازات الدخول	**Access Rights / Privileges**	تحدد حقوق دخول (أو امتيازات الدخول) المستخدم إلى أصل معلوماتي الإجراءات التي يُسمح للمستخدم القيام بها عند الدخول إلى الأصل المعلوماتي.
أصل	**Asset**	الأصل كل ما له قيمة بالنسبة للمؤسسة.
مالك الأصل	**Asset Owner**	الشخص أو الجهة المفوّضة باتخاذ قرارات فيما يتعلق بالأصل.
سجل التدقيق (ملفات الأنشطة)	**Audit Logs (log files)**	الملف حيث يتم تسجيل الأحداث التي تجري في النظام.
أصالة	**Authenticity**	ضمان بان الطرف هو/هي بالفعل من هو الشخص المزعوم.
توافر	**Availability**	خاصية إتاحة الدخول والاستخدام عند الحاجة من قبل جهة مفوّضة.
تحليل الآثار على العمل	**Business Impact Analysis**	إحدى عمليات العمل حيث يتم التنبؤ بعواقب الخسارة المحتملة لسرية الأصل أو تكامله أو توافره.
سرية	**Confidentiality**	خاصية عدم توفير المعلومات أو إفشائها إلى أشخاص، او جهات أو عمليات غير مفوّضة.
آلية تحكّم (احتياطات)	**Control (measure)**	وسيلة لإدارة المخاطر، بما في ذلك السياسات، والإجراءات، والإرشادات ...إلخ، وتكون ذات طبيعة إدارية أو تقنية أو قانونية.
إخفاء	**Cryptography**	الإخفاء ضمن سياق هذا الكتيّب، هو النظام الكلي الذي يدعم ويدير تشفير وفك تشفير المعلومات.
تشفير	**Encryption**	تحويل النص القابل للقراءة إلى صيغة غير مقروءة.
حادثة	**Incident**	أي حدث (نشاط) تتوفر فيه القدرة على الإضرار بأمن أصل أو أكثر من أصول المؤسسة.
تصنيف المعلومات	**Information Classification**	عملية ترتيب المعلومات وفقاً لأهميتها بالنسبة للعمل.
تسهيلات/مرافق معالجة المعلومات	**Information Processing Facilities**	أي نظام أو خدمة أو بنية تحتية لمعالجة المعلومات، أو الموقع الذي يحتويها.
أمن المعلومات	**Information Security**	المحافظة على سرية وتكامل وتوافر المعلومات؛ كما يمكن أن تشترك في ذلك خصائص أخرى مثل الأصالة، المساءلة، عدم التنصّل، والموثوقية.
تسجيل (تسجيل الأحداث)	**Logging (Event Logging)**	توليد وتخزين معلومات محددة بخصوص أنشطة (أحداث) جرت على النظام.
برنامج خبيث (رموز برمجية خبيثة)	**Malware (malicious code)**	برنامج يُستخدم في التشويش على تشغيل الحاسب الآلي، وجمع معلومات حساسة، أو الحصول على دخول غير مصرح به إلى أنظمة الحاسب الالي.
اختبار اختراق	**Penetration Testing**	محاولة منضبطة لاختراق نظام الحاسب الالي، ومحاكاة الطرق والتقنيات التي ينفذها المخترق ذو النوايا السيئة، من أجل تحديد كيفية قيام المهاجم الحقيقي باختراق النظام؛ وما هو الضرر الذي يمكن أن يتسبب به.

المصطلح	Term	التعريف
سياسة	**Policy**	خطة عمل لتوجيه القرارات والإجراءات. وقد ينطبق المصطلح على القطاع الحكومي، وعلى مؤسسات ومجموعات القطاع الخاص، والإفراد. تشمل السياسة تحديد البدائل المختلفة، مثل البرامج أو أولويات الإنفاق، والاختيار من بينها على أساس الأثر الذي قد تتركه.
نقطة الاستعادة المستهدفة	**Recovery Point Objective**	الحد الأقصى المقبول لخسارة البيانات، مقاساً بالوقت، في أعقاب وقوع كارثة.
وقت الاستعادة المستهدف	**Recovery Time Objective**	الحد الأقصى المرغوب للوقت والذي يسمح به بين الفشل غير المتوقّع أو كارثة، واستئناف المستويات الطبيعية للتشغيل أو الخدمة.
خطر	**Risk**	الخطر هو مزيج من احتمال وقوع حادث وعواقبه فيما لو وقع.
الفصل بين الواجبات	**Segregation of Duties**	آليات تحكّم أمنية وقائية تقتضي وجود أكثر من شخص لإنجاز عملية حيوية.
طرف ثالث	**Third Party**	ذلك الشخص أو الجهة الذي يُنظر إليه على أنه مستقل عن الأطراف المشاركة فيما يختص بالقضية مدار البحث.
تهديد	**Threat**	تهديد يتوفر فيه احتمال التسبب بحادثة غير مرغوب بها قد تسفر عن الإضرار بالنظام.
نقطة ضعف أمنيّة	**Vulnerability**	وهي عبارة عن ثغرة في أحد الأصول.

10.2 الاختصارات

الاختصار	المعنى الإنجليزي	المعنى بالعربي
BCP	Business Continuity Plan	خطة استمرارية الأعمال
BIA	Business Impact Analysis	تحليل التأثيرات على العمل
CCTV	Closed Circuit Television	دائرة تلفزيونية مغلقة
IPS	Intrusion Prevention System	نظام منع الاختراق
IRT	Incident Response Team	فريق الاستجابة للحوادث
ISO	International Standardization Organization	المنظّمة الدوليّة للمعايير
ISSC	Information Security Steering Committee	لجنة توجيه أمن المعلومات
ISMS	Information Security Management System	نظام إدارة أمن المعلومات
ITDL	IT and Distance Learning Deanship	عمادة تقنية المعلومات والتعليم عن بعد
RA	Risk Assessment	تقييم مخاطر
RPO	Recovery Point Objective	نقطة الاستعادة المستهدفة
RTO	Recovery Time Objective	زمن الاستعادة المستهدف
SAT	Security Awareness Training	التدريب على التوعية بأمن المعلومات
SLA	Service Level Agreement	اتفاقية مستوى خدمة
NDA	Non-Disclosure Agreement	اتفاقية المحافظة على المعلومات السرية
SoD	Segregation of Duties.	الفصل بين الواجبات
UPS	Uninterruptible Power Supply	مصدر للطاقة الاحتياطية