# سياسة تصنيف الأصول وترميزها

V1.1

## تفاصيل الوثيقة

| | |
|---|---|
| اسم الوثيقة | سياسة تصنيف الأصول وترميزها |
| تصنيف الوثيقة | للاستخدام الداخلي |
| رقم آخر إصدار | 1.1 |
| نوع الوثيقة | تحديث |
| مالك الوثيقة | إدارة الأمن السيبراني |
| مرجعية الوثيقة | ISO/IEC 27001:2013<br>NCA ECC-1:2018 |

## جدول التعديلات على الوثيقة

| وصف التغيير | تم الإعداد بواسطة | رقم الإصدار | التاريخ |
|---|---|---|---|
| **إعداد الوثيقة** | إدارة الأمن السيبراني | 1.0 | 02-سبتمبر-2021 |
| **تحديث الوثيقة** | إدارة الأمن السيبراني | 1.1 | 13-مارس-2022 |
| | | | |

## جدول مراجعة الوثيقة

| تمت المراجعة بواسطة | التاريخ | التوقيع | تاريخ المراجعة القادم |
|---|---|---|---|
| **مدير إدارة الأمن السيبراني " م. خالد إبراهيم الفيفي"** | 2021/10/10 | | مارس 2022 |
| **نائب مدير إدارة الأمن السيبراني "سامر محمد أحمد الضويمر"** | 2022/5/26 | | مارس 2023 |

| | | | |
|---|---|---|---|
| | | | |

**جدول اعتماد الوثيقة**

| تم الاعتماد بواسطة | التاريخ | التوقيع | تاريخ المراجعة القادم |
|---|---|---|---|
| **رئيس جامعة تبوك** | 2021/10/11 | | مارس 2022 |
| **رئيس جامعة تبوك** | 2022/5/29 | | |
| | | | |

# جدول المحتويات

## 1. المقدمة

تُمَثِّل هذه الوثيقة سياسة تصنيف الأصول وترميزها الخاصة بجامعة تبوك والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من تِسعة أقسام رئيسية لِتَشمل هذه المُقَدِمَة يليها الغَرض، والنطاق، والأدوار والمسؤوليات، وبنود السياسة، والمرجعيات، والالتزام، ومعايير الاستثناءات، وأخيراً المصطلحات والتعريفات.

على جَمِيع المستخدمين القيام بالقراءة المُتأنِية والفهم الجيد والالتزام الكامل بسياسة تصنيف الأصول وترميزها. وفي حالة عدم وضوح أيا من معلومات هذه الوثيقة أو لأي جزءٌ منها، فنأمل التواصل مع إدارة الأمن السيبراني لشرحها وتوضيحها.

تُعَدُ إدارة الأمن السيبراني بالجامعة هي المالكة لِتلك الوثيقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على إدارة الأمن السيبراني مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، أو يجوز أيضاً تحديثها فور حُدوث أى تعديلات أو تغييرات تَتَعلَّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تَغيير رقم إصدار الوثيقة حال القِيام بأى تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ اللجنة الإشرافية للأمن السيبراني بالجامعة.

## 2. الغرض

تَهدُف هذه السياسة إلى ضمان وُجود سِجِل دَقيق ومُفصَّل عن الأصول المعلوماتية والتقنية بهدف دعم مُتطلبات الأمن السيبراني التشغيلية الخاصة بالجامعة حتى تتمكن من الحفاظ على سِرِّية وسلامة وتوافر البيانات والمعلومات والأصول المعلوماتية والتقنية، وكذلك تحديد مسئوليات الحماية المناسبة وفقا لسياسات وإجراءات الجامعة والمُتطلبات التشريعية والتنظيمية ذات العلاقة.

## 3. النطاق

تنطبق هذه الوثيقة على كافة الأصول المعلوماتية والتقنية والخدمات المقدمة وعلى جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجهات داخل جامعة تبوك مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية، الاجتماعات، والاتصالات عبر وسائل التواصل والتطبيقات، ورسائل البريد الإلكتروني، والبيانات المخزنة على وسائط إلكترونية، وأشرطة الصوت أو الفيديو، والخرائط، والصور الفوتوغرافية، والمخطوطات، والوثائق المكتوبة بخط اليد، البيانات المخزنة في أنظمة الجامعة مثل نظام مسار، نظام إدارة التعلم الالكتروني (البلاكبورد)، نظام القبول والتسجيل(E-Register) ، البوابة الإلكترونية وجميع أنظمة الجامعة وأي شكل آخر من أشكال البيانات المسجلة، وكذلك كافة مستخدميها من الموظفين سواء كانوا يعملون بصفة دائمة أو مؤقتة، أو يعملون بدوام كامل أو دوام جزئي، أو متعاقدين كموظفي شركات الإسناد الخارجي. وكذلك مستخدمي وموظفي جميع الأطراف الخارجية كالمقاولين والموردين والشركات الاستشارية والجهات الحكومية وشركات الخدمات المُدارة والشركات والجهات الخاصة بالاستضافة والحوسبة السحابية وغيرها.

## 4. الأدواروالمسؤوليات

| المسؤول | الإعداد والتحديث والمراجعة | الاعتماد | النشر | الالتزام والتطبيق |
|---|---|---|---|---|
| اللجنة الإشرافية للأمن السيبراني | | | | |
| إدارة الأمن السيبراني | | | | |
| جميع موظفي الجامعة وجميع الأطراف المعنية الداخلية والخارجية | | | | |

## 5. بنود السياسة

### 5.1 تصنيف البيانات والمعلومات والأصول المعلوماتية والتقنية

5.1.1 يجب على إدارة الأمن السيبراني تحديد مستويات التصنيف المناسبة لجميع البيانات والمعلومات والأصول المعلوماتية والتقنية أثناء تخزينها ومعالجتها ونقلها ومشاركتها والتخلص منها بشكل آمن.

5.1.2 يجب على جميع المستخدمين والموظفين الالتزام بمستويات التصنيف المحددة.

5.1.3 يجب مراجعة تصنيف البيانات والمعلومات والأصول المعلوماتية والتقنية مرة واحدة على الأقل سنوياً أو في حالة حدوث أي تغييرات جوهرية.

5.1.4 يجب على إدارة الأمن السيبراني تحديد مستويات التصنيف بُناءً على حساسية وأهمية وسِرّية وقيمة البيانات ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سرية البيانات، والمعلومات، والأصول المعلوماتية، والتقنية.

5.1.5 يجب تصنيف كافة البيانات والمعلومات والأصول المعلوماتية والتقنية على أساس مخطط التصنيف التالي:

- **سِرّي للغاية:** ينطبق فقط على البيانات والمعلومات والأصول المعلوماتية والتقنية التي قد تتضمن معلومات حساسة، أو قيّمة للغاية، أو ذات حق ملكية، أو شخصية على حد سواء، والتي لن يتم الكشف عنها خارج الجامعة أو داخلها دون إذن كتابي صريح من مالك البيانات والمعلومات. إذا تم الكشف عنها أو الوصول إليها، من قِبَل أشخاص غير مُصرَّح لهم، قد تؤثر سلبًا على المصالح العامة أو الخاصة، أو يكون لها تأثير

سلبي على الحياة الاجتماعية للأفراد وتؤثر سلبيًا على صورة الجامعة أو سمعتها أو قد يؤدي اختراقها او الوصول لها دون اذن الى توجيه اتهامات جنائية وغرامات قانونية ضخمة أو التسبب في ضرر لا يمكن اصلاحه للجامعة. لا يمكن الوصول إلى هذه الوثائق، خلال فترة التقييد، إلا من قِبَل كبار المسؤولين المعنيين، أو من قِبَل المحاكم التي لها اختصاص قضائي في القضايا التي تتعلق بمصالح الأمن القومي وإلى الحد اللازم للبت في هذه القضايا .

- **سري:** ينطبق فقط على البيانات والمعلومات والأصول المعلوماتية والتقنية التي يجب الحصول على إذنا و/أو تصريحا محددا وموافقة مالك البيانات والمعلومات قبل الإفصاح لأي شخص داخل الجامعة أو خارجها، يجب تطبيق مستوى معقول من الضوابط الأمنية على البيانات المقيدة.
- **مقيد:** ينطبق فقط على البيانات والمعلومات والأصول المعلوماتية والتقنية التي قد يؤدي إفشاءها إلى تأثير طفيف ومحدود على العمل ويُمكِن مشاركتها وإبلاغها داخليًا داخل الجامعة. يجب الحصول على موافقة مالك البيانات والمعلومات قبل الإفصاح لأي شخص خارج الجامعة بصفة خاصة، كما يمكن تصنيف البيانات المصنفة على مستوى مقيد إلى مستويات فرعية بناء على نطاق الأثر على النحو التالي:
  - مقيد – مستوى (أ): إذا كان نطاق الأثر على مستوى قطاع كامل أو نشاط اقتصادي عام.
  - مقيد - مستوى (ب): إذا كان نطاق الأثر على مستوى أنشطة عدة جهات أو على مصالح مجموعة من الأفراد.
  - مقيد - مستوى (ج): إذا كان نطاق الأثر على مستوى أنشطة جهة واحدة أو مصالح فرد معين.
- **عام:** ينطبق على البيانات والمعلومات التي قد يتم توزيعها بشكلٍ واسع دون التسبب في إلحاق الضرر بالجامعة وموظفيها وعملائها. يجب على مالك البيانات والمعلومات بالجامعة الموافقة المسبقة على استخدام هذا التصنيف. وقد يتم الإفصاح عن هذه المستندات أو تمريرها إلى أشخاص خارج الجامعة. ينطبق هذا التصنيف على الموضوعات العامة غير المُصنَّفة والتي تم تداولها وكشفها لأي شخص. تتعلق هذه الوثائق، على سبيل المثال لا الحصر، بالقوانين والأنظمة والخطط والبرامج والإحصاءات والدراسات والتقارير الإحصائية.

5.1.6 يجب أن تحدد إدارة الأمن السيبراني بالجامعة معيار التقييم للمساعدة في تقييم جميع الأصول المعلوماتية والتقنية بالجامعة وفقًا لمستويات السِرّية والسلامة والتوافر (CIA) للمعلومات ذات العلاقة، وإذا اختلفت مستويات CIA السرية والتوافر والسلامة لأي أصول؛ سيُؤْخَذْ بقيمة، المعلومات والأصول ذات العلاقة، الأعلى قيمة.

5.1.7 سيحدِّد الجدول التالي المستويات المختلفة للسِرّية والسلامة والتوافر (CIA):

| الأهداف الأمنية | مستوى التأثير | | |
|---|---|---|---|
| | منخفض | متوسط | مرتفع |
| **السِرّية**<br>الحفاظ على القيود، المُصرَّح بها، على الوصول إلى المعلومات والإفصاح عنها، بما في ذلك وسائل حماية المعلومات | إفشاء، المعلومات غير المُصرَّح به، مُتوقَّع ان يكون له تأثير سلبي محدود على سَيْرْ العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين | إفشاء المعلومات غير المُصرَّح به، مُتوقَّع أن ينتج عنه تأثيرات خطيرة على سَيْرْ العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين | إفشاء المعلومات غير المُصرَّح به، المُتوقَّع أن ينتج عنه تأثير حاد وكارثي على سير العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين. |
| **السلامة**<br>الوقوف ضد أي، تعديل أو تدمير للمعلومات بشكل غير مناسب، ويشمل ضمان عدم الإنكار والصحة | التعديل أو التدمير غير المُصرَّح به، مُتوقَّع ان يكون له تأثير سلبي محدود على سَيْرْ العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين | التعديل أو التدمير غير المُصرَّح به، مُتوقَّع أن يَنتُج عنه تأثيرات خطيرة على سَيْرْ العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين | التعديل أو التدمير غير المُصرَّح به، المُتوقَّع أن ينتج عنه تأثيرات حادة وكارثيةِ الأثر على سَيْرْ العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين. |
| **التو افر** | تعطيل الوصول إلى، المعلومات أو نظم المعلومات، وعدم القدرة على استخدامها، مُتوقَّع ان يكون له تأثير سلبي محدود على سَيْرْ العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين | تعطيل الوصول إلى، المعلومات أو نظم المعلومات، وعدم القدرة على استخدامها، مُتوقَّع أن ينتج عنه تأثيرات خطيرة على سَيْرْ العمل بالجامعة وكذلك | تعطيل الوصول إلى، المعلومات أو نظام معلومات، وعدم القدرة على استخدامها، المُتوقَّع أن ينتج عنه تأثير حاد وكارثي على سير العمل بالجامعة وكذلك الأصول والمستخدمين والموظفين. |

| | | | |
|---|---|---|---|
| | | الأصول والمستخدمين والموظفين | |

## قياس مستوى الأثر:

| | |
|---|---|
| فئة الأثر الرئيسة | مصلحة الجامعة |
| فئة الأثر الفرعية | سمعة الجامعة |
| الاعتبارات | هل ستخضع المعلومات لاهتمام وسائل الإعلام المحلية أو الدولية؟ هل ستعطي انطباع سلبي؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تتأثر السمعة بشكل كبير. | تتأثر السمعة إلى حد ما. | لا تتأثر السمعة. | لا يوجد تأثير |

| | |
|---|---|
| فئة الأثر الرئيسة | مصلحة الجامعة |
| فئة الأثر الفرعية | اقتصاد الجامعة |
| الاعتبارات | هل يؤدي الكشف عن المعلومات إلى خسائر اقتصادية على المستوى الجامعي؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تأثير طويل المدى على الاقتصاد مع انخفاض لا يُمكن تداركه في الناتج الإجمالي أو أسعار الأسواق المالية أو نسبة البطالة أو القوة الشرائية أو المؤشرات الأخرى ذات الصلة؛ مما ينعكس سلباً على مرافق الجامعة | تأثير طويل المدى على الاقتصاد مع انخفاض يُمكن تداركه في الناتج المحلي الإجمالي ونسبة البطالة أو أسعار الأسواق المالية أو القوة الشرائية؛ مما ينعكس سلباً على قطاع واحد أو أكثر. | تأثير بسيط على الاقتصاد مع انخفاض يُمكن تداركه في وقت قصير في الناتج المحلي الإجمالي، ومعدل العمالة أو أسعار الأسواق المالية أو القوة الشرائية؛ مما ينعكس سلباً على قطاع واحد فقط. | |

| | |
|---|---|
| فئة الأثر الرئيسة | مصلحة الجامعة |
| فئة الأثر الفرعية | مهام الجامعة |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى الحد من إمكانية الجامعة من تنفيذ عملياتها ومهامها اليومية؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| عدم قدرة الجامعة على أداء مهامها وعملياتها الرئيسة لفترة طويلة. | عدم قدرة الجامعة على أداء واحدة أو أكثر من مهامها الرئيسة لفترة قصيرة. | عدم قدرة الجامعة على أداء مهمة واحدة أو أكثر من المهام غير الرئيسة لفترة قصيرة. | لا يوجد اثر |

| | |
|---|---|
| فئة الأثر الرئيسة | أنشطة الجامعة |
| فئة الأثر الفرعية | أرباح الجامعة |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى خسائر مالية أو إفلاس الجامعة، أو احتمالية الاحتيال، وتحويلات الأموال غير القانونية، والمصادرة غير القانونية للأصول؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تأثير سلبي كبير على الجامعة إلى الحد الذي يتسبب في الإضرار بالمصالح. | تكبد الجهة خسائر مالية فادحة مما قد يؤدي إلى الإفلاس. | ضرر محدود يتمثل في خسارة مالية محدودة للجهة أو لأيٍ من أصولها. | لا يوجد تأثير. |

| | |
|---|---|
| فئة الأثر الرئيسية الاعتبارات | أنشطة الجامعة |
| فئة الأثر الفرعية | مهام الجامعة |
| | هل سيؤدي الكشف عن المعلومات إلى حدوث أضرار على الجامعة؟ هل سيؤدي ذلك إلى فقدان الدور الريادي التي تتمتع به الجهة أو خسارة أيٍ من أصولها؟ هل سيؤدي ذلك إلى إنهاء عقود عددٍ كبيرٍ من الموظفين؟ هل سيؤثر على القدرة التنافسية للجامعة؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية. | عدم إمكانية الجهة من القيام بمهامها الرئيسة ،وفقدان القدرة على التنافسية إلى حد كبير. | عدم إمكانية الجهة من أداء إحدى مهامها الرئيسة، وفقدان القدرة على التنافسية بشكل محدود. | لا يوجد تأثير على أنشطة الجهات. |

| | |
|---|---|
| فئة الأثر الرئيسة | الأفراد |
| فئة الأثر الفرعية | صحة/ سلامة الأفراد |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى إفشاء أسماء أو مواقع أشخاص وما إلى ذلك؟ على سبيل المثال، أسماء وبيانات منسوبي الجامعة |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| خسارة عامة أو فادحة في الأرواح، وفقدان حياة فرد أو مجموعة من الأفراد. | ضرر جسيم أو إصابة تهدد حياة الفرد. | إصابة بسيطة دون أي خطر يهدد حياة أو صحة الفرد. | لا يوجد تأثير على الأفراد |

| | |
|---|---|
| فئة الأثر الرئيسة | الأفراد |
| فئة الأثر الفرعية | الخصوصية |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى انتهاك خصوصية الأفراد في جامعة تبوك؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| الكشف عن البيانات الشخصية لشخصية مهمة في جامعة تبوك. | الكشف عن البيانات الشخصية لشخصية مهمة في جامعة تبوك. | الكشف عن البيانات الشخصية للفرد في جامعة تبوك. | لا يوجد تأثيرعلى الأفراد في جامعة تبوك |

| | |
|---|---|
| فئة الأثر الرئيسة | الأفراد |
| فئة الأثر الفرعية | صحة/ سلامة الأفراد |
| الاعتبارات | هل سيؤدي ذلك إلى انتهاك أي حقوق ملكية فكرية في جامعة تبوك؟ |

| مستوى الأثر |
|---|

| | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| مما يؤثر على المصلحة الوطنية. | | | |

| | |
|---|---|
| فئة الأثر الرئيسة | البيئة |
| فئة الأثر الفرعية | الموارد البيئية |
| الاعتبارات | هل سيتم استخدام هذه المعلومات لتطوير خدمة أو منتج يمكن أن يؤدي إلى تدمير الموارد البيئية أو الطبيعية ؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تأثير كارثي لا يمكن تداركه على البيئة أو الموارد الطبيعية. | تأثير طويل المدى على البيئة أو الموارد الطبيعية. | تأثير قصير المدى أو محدود على البيئة أو الموارد الطبيعية. | لا يوجد تأثير على البيئة. |

5.1.8 إذا تم الجمع بين أي بيانات أو معلومات ذات تصنيفات مختلفة، فيجب الأخذ بالتصنيف الأكثر تقييداً على جميع البيانات.

5.1.9 بشكل افتراضي، يجب معاملة جميع بيانات الجامعة التي لم يتم تصنيفها بشكل واضح على أنها بيانات سرية.

5.1.10 بالنسبة لجميع البيانات والمعلومات والأصول المعلوماتية والتقنية الجديدة والحالية، يكون المالك مسؤولاً عن اختيار التصنيف المناسب ليستخدمه جميع رعاة الأصول والمستخدمين والموظفين الذين يقومون بإنشاء معلومات التشغيل أو تجميعها أو تعديلها.

5.1.11 يجب إعادة تصنيف أي وسائط تخزين قابلة للكتابة يمكن تعديلها، مثل القرص المرن والشريط المغناطيسي والأقراص المضغوطة والأقراص المدمجة ووسائل تخزين المعلومات كالقرص الصلب ووسائل التخزين المتنقلة التي تحتوي على أي بيانات أو تطبيقات سِرّية، إلى مستوى سِرّي.

5.1.12 عند تسجيل معلومات، ذات تصنيف أعلى، على أية وسائط تخزينية، وكذلك في حالة إذا تم نقلها إلى وسائط ذات تصنيف أقل، فيجب ترقية الوسائط ذات التصنيف الأدنى بحيث يعكس تصنيفها أعلى مستوى تصنيف للبيانات والمعلومات المخزنة.

5.1.13 يجوز لمالك البيانات والمعلومات والأصول المعلوماتية والتقنية، رفع التصنيف أو خفض التصنيف المُطبَّق، عن طريق تغيير مُلصَق التصنيف وإخطار جميع الموظفين ورعاة الاصول والمستخدمين ذوي العلاقة، وما إلى ذلك

5.1.14 الأصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي والأمني) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

5.1.15 يتم تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة.

5.1.16 يتم الفصل بين مهام ومسؤوليات العاملين في جامعة تبوك - فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها - بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤولية.

5.1.17 يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين في جامعة تبوك.

5.1.18 يتم تقييد إدارة صلاحيات العاملين في جامعة تبوك على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناطة بهم.

5.1.19 يجب تصنيف البيانات التي لم يتم تصنيفها وقت إصدار هذه السياسة خلال فترة زمنية محددة بموجب خطة عمل تعدها جامعة تبوك ويتم اعتمادها من المسؤول الأول بالجامعة.

[ISO/IEC 27001:2013, A.8.2.1]

## 5.2 ترميز البيانات والمعلومات والأصول المعلوماتية والتقنية

5.2.1 يجب أن تكون عملية الترميز متوافقة مع التسمية المتعارف عليها والمعتمدة داخل الجامعة، ويجب أن تتطابق عملية الترميز مع مخطط تصنيف الأصول المعلوماتية والتقنية.

5.2.2 يجب تخزين، جميع المستندات المطبوعة التي تحتوي على بيانات ومعلومات مصنفة على أنها "سِرّية" أو "سِرّية للغاية"، في أدراج أو خزانات مقفلة أثناء عدم تواجد الموظف في المكتب، كما يجب إغلاق أي مكتب يحتوي على مستندات سِرّية أو "سِرّية للغاية".

5.2.3 يجب مُراعاة وَضْع المُلصَقات، على المستندات وعناصر الأجهزة والوسائط القابلة للإزالة، بعد تحديد التصنيفات المناسبة وفقًا لسياسة تصنيف الأصول وترميزها بالجامعة.

5.2.4 لا يجوز تسليم الوسائط التي تحتوي على معلومات مصنفة على أنها "سِرّية للغاية" إلى أي جهة خارجية أو طرف خارجي، ما لم تُصرّح بذلك الإدارة وتوافق عليها بَعْد إبداء المبررات المنطقية لذلك.

5.2.5 لا يجوز إرسال المعلومات السِرّية غير المشفرة من خلال أي طَرَف خارجي بما في ذلك، على سبيل المثال لا الحصر، شركات النقل والخدمات البريدية ومقدمي خدمات الإنترنت. وذلك لضمان عدم وقوع المعلومات السِرّية في أيدي أي أطراف غير مُصرَّح لها.

5.2.6 يُمنَع عمل نسخ إضافية أو طباعة نسخ إضافية من المعلومات السِرّية للغاية دون الحصول على موافقة مسبقة من مالكي البيانات والمعلومات.

5.2.7 في حالة عمل نسخ إضافية من المعلومات السِرّية للغاية، فإنه يجب تسجيل عدد النُسَخ الإضافية ومستلمي هذه النُسَخ في سِجِّل، ويجب إخطار كل الموظفين أو الجهات التي سوف تقوم باستلام هذه النسخ بأنه لن يتم التوزيع الإضافي أو النسخ الإضافي إلا بعد الحصول على الموافقة من مالك البيانات والمعلومات.

5.2.8 يجب تواجد الأشخاص المُصرَّح لهم بفحص المعلومات التي يتم طباعتها في حالة طباعة معلومات "سِرّية للغاية"، وذلك إذا لم يتم استخدام ضوابط الوصول المادي، لمنع الأشخاص غير المُصرَّح لهم من دخول المنطقة المحيطة بالطابعة.

[ISO/IEC 27001:2013, A.8.2.2]

## 5.3 التعامل مع البيانات والمعلومات والأصول المعلوماتية والتقنية

5.3.1 يجب تطوير وتطبيق أساليب معالجة البيانات والمعلومات والأصول المعلوماتية والتقنية من أجل حمايتها من الإفشاء غير المُصرَّح به أو سوء الاستخدام. كما يجب أن تكون أساليب وإجراءات معالجة البيانات والمعلومات وضوابط الحماية المُعيَّنَة متوافقة مع تصنيفها.

5.3.2 يجب وضع الضوابط التالية في الاعتبار عند التعامل مع البيانات والمعلومات:

- التعامل مع كافة الوسائط ووضع العلامات عليها، بالإضافة تُطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقاً لكل مستوى من مستويات التصنيف.
- فرض قيود على الوصول لتحديد أي أفراد غير مُصرَّح لهم بحيث:
  - يُمنح الوصول – المنطقي والمادي - للبيانات بناءً على مبدأ "الحد الأدنى من الامتيازات والحاجة إلى المعرفة"
  - يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين بجامعة تبوك.
- الاحتفاظ بسجل رسمي للمستلمين، المعتمدين، للبيانات.
- التأكد من اكتمال إدخال البيانات، وإتمام المعالجة بشكل صحيح، وأنه تم تطبيق التحقق من صحة المخرجات.
- الحفاظ على توزيع البيانات عند الحد الأدنى، خاصة فيما يتعلق بأي بيانات ومعلومات سِرّية.
- مراجعة قوائم التوزيع وقوائم المستلمين المعتمدين مرة واحدة على الأقل كل عام.
- تُستخدم البيانات المصنفة وفقاً لمتطلبات مستويات التصنيف، على سبيل المثال، يتم تقييد استخدام البيانات المصنفة "سرية للغاية" على مواقع محددة سواء مادية – كالمكاتب – أو افتراضية باستخدام ترميز الأجهزة أو تطبيقات خاصة

- لا تُترك البيانات المصنفة على أنها "سري للغاية" و" سري" و "مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة.
- يجب حماية البيانات المصنفة على أنها "سري للغاية" و" سري" و "مقيّد" غير المراقبة أثناء تخزينها مادياً أو إلكترونياً باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

[ISO/IEC 27001:2013, A.8.2.3]

## 5.4 إلغاء التصنيف (رفع السرية)

يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى الأصلي للتصنيف.

في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.

5.4.1 يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، كما يجب تسجيلها في سجل أصول البيانات، قد تتضمن هذه العوامل ما يلي:

- فترة زمنية محددة بعد إنشاء البيانات أو تلقيها على سبيل المثال: عامين بعد الإنشاء.
- فترة زمنية محددة بعد اتخاذ أخر إجراء على البيانات على سبيل المثال: ستة أشهر من تاريخ آخر استخدام.
- بعد انقضاء تاريخ محدد على سبيل المثال، من المقرر مراجعتها في 1 يناير 2024
- بعد ظروف أو أحداث معينة تأثيراً مباشراً على البيانات على سبيل المثال: إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية.
- يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيداً عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

[SDAIA, 2021]

## 5.4 الخطوات اللازمة لتصنيف البيانات

**الخطوة 1 - تحديد جميع بيانات الجهة**

تتمثل الخطوة الأولى التي تتخذها جامعة تبوك في جرد وتحديد جميع البيانات التي تمتلكها الجامعة وفق نموذج تصنيف البيانات (نموذج أ) ونموذج تصنيف الوثائق (نموذج ب) (مرفق النماذج في الملحقات).

**الخطوة 2 - تعيين مسؤول تصنيف البيانات**

على كل جهة داخل الجامعة تشكيل لجنة داخلية أو شخص يتولى مسؤولية عملية التصنيف وتحديد جميع البيانات والوثائق بالجهة، ويجب أن تتحمل الجهة المسؤولية حيال إجراء التصنيف الأولي.

**الخطوة 3 - إجراء عملية تقييم الأثر**

1. يجب على الجهة اتباع الخطوات اللازمة لعملية تقييم الأثر وفق (نموذج أ) الذي يترتب على:
   - الإفصاح عن هذه البيانات أو الوصول غير المصرح به إليها
   - إجراء تعديل على هذه البيانات أو إتلافها أو كليهم عدم الوصول إلى هذه البيانات في الوقت المناسب
2. تبدأ عملية تقييم الأثر بتطبيق مبدأ "الأصل في البيانات الإتاحة" (في المجال التنموي) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية؛ السرية للغاية، و (في المجال السياسي والأمني) ما لم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف.

**الخطوة- 3أ - تحديد فئة الأثر:**

1. يتمثل العنصر الأول من عملية تقييم الأثر في تحديد الفئة الرئيسة والفرعية للأثر المحتمل في أيٍ من الفئات الرئيسة التالية:
   - مصلحة الجامعة

- أنشطة جهات الجامعة
- صحة أو سلامة منسوبي الجامعة
- الموارد البيئية

**الخطوة 3-ب - تحديد مستوى الأثر:**

1. **يُشير العنصر الثاني إلى أنه يتعين على الجهة أن تحدد لكل أثر محتمل مستوى معين يعتمد تحديد المستوى على الآتي:**

- مدة الأثر وصعوبة السيطرة على الضرر
- فترة تدارك وإصلاح الأضرار بعد وقوعها
- حجم الأثر على مستوى وطني، مناطقي، عدة جهات، جهة واحدة، عدة أفراد... إلخ

2. **تحدد هذه المعايير مستويات الأثر الأربعة:**

- **عالي:** يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرارٍ جسيمة أو خطيرة للغاية على المدى الطويل لا يمكن تداركها أو إصلاحها.
- **متوسط:** يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرار جسيمة أو خطيرة يصعب السيطرة عليها.
- **منخفض:** يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى أضرارٍ محدودة يمكن السيطرة عليها أو أضرار متقطعة على المدى القصير يمكن السيطرة عليها.
- **لا يوجد أثر:** لا يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى أي ضرر على المدى الطويل أو القصير.

3. **يجب أن تكون جميع الأضرار المحتملة والمحددة خلال عملية تقييم الأثر محددة وقائمة على أدلة، في محاولة للحد من التقديرات الشخصية للمكلف بإجراء تصنيف البيانات.**

4. **يحدد ممثل بيانات الأعمال مستوى تصنيف البيانات بناءً على الآثار المحددة ومستوياتها:**

- **عالٍ:** تُصنف البيانات باعتبارها "سرية للغاية".
- **متوسط:** تُصنف البيانات على أنها "سرية".
- **منخفض:** يلزم إجراء مزيدٍ من التقييمات (يرجى الاطلاع على الخطوة 4 و5).
- **لا يوجد أثر:** تُصنف البيانات على أنها بياناتٍ "عامة".

5. يوجد وصف مفصل للاعتبارات الرئيسة لكل فئة من فئات الأثر ومستواه في الجدول (2) "فئات ومستويات تقييم أثر تصنيف البيانات"
6. يجب الأخذ بعين الاعتبار الخطوتين 4 و5 عندما يكون مستوى الأثر المحدد منخفض.
7. يتم الانتقال إلى الخطوة 6 عندما تُصنف البيانات على أنها "سرية للغاية" أو "سرية" أو "عامة."

**الخطوة 4 – تحديد الأنظمة ذات العلاقة (فقط إذا كان مستوى الأثر منخفضاً).**

1. يجب إجراء تقييمات إضافية إذا كان مستوى الأثر المحدد "منخفض" وذلك بهدف زيادة مستوى تصنيف البيانات المصنفة على أنها بيانات "عامة" إلى الحد الأقصى.
2. يجب على ممثل بيانات الأعمال في جامعة تبوك، دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربية السعودية مثل نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية ... الخ وإذا كان الإفصاح عن البيانات مخالفاً للأنظمة، فيجب حينها تصنيف البيانات على أنها بيانات "مقيّدة"، بخلاف ذلك يتعين على ممثل بيانات الأعمال مواصلة تنفيذ الخطوة 5.

**الخطوة 5 - الموازنة بين مزايا الإفصاح عن البيانات والآثار السلبية (فقط إذا كانت الإجابة على الخطوة 4 "لا.)**

1. التأكد من مستوى الأثر المنخفض وضمان أن الإفصاح لن يكون انتهاكاً لأي نظام نافذ.
2. يجب أيضاً تقييم المزايا المحتملة للإفصاح عن مثل هذا البيانات والتأكد مما إذا كانت هذه المزايا ستفوق الآثار السلبية أم لا، وتشمل المزايا المحتملة استخدام البيانات لتطوير خدمات جديدة ذات قيمة مضافة، أو زيادة شفافية العمليات الحكومية أو زيادة مشاركة الأفراد مع الحكومة.

3. إذا كانت المزايا أكبر من الآثار السلبية، تصنف البيانات على أنها "عامة".
4. إذا كانت المزايا أقل من الآثار السلبية، تصنف البيانات على أنها "مقيّدة".

**الخطوة 6 - مراجعة مستوى التصنيف**

يجب أن تفحص إدارة الأمن السيبراني جميع البيانات المصنفة لضمان أن يكون مستوى التصنيف المحدد من جانب الجهة هو الأنسب.

**الخطوة 7 - تطبيق الضوابط المناسبة**

1. تتمثل الخطوة الأخيرة من عملية تصنيف البيانات في حماية جميع البيانات وفقاً لمستوى التصنيف عن طريق تطبيق عناصر التحكم ذات الصلة (راجع "ضوابط تصنيف البيانات").
2. يتم الانتهاء من عملية التصنيف عند تصنيف جميع البيانات التي تملكها جامعة تبوك والتحقق من مستويات التصنيف وتطبيق الضوابط ذات الصلة.
3. بعد تصنيف البيانات على نحوٍ صحيح، يمكن للجهات في جامعة تبوك مشاركتها مع جهات أخرى، أو إتاحتها ونشرها بصفتها بيانات مفتوحة عند تصنيفها بيانات "عامة".

[SDAIA, 2021]

## 5.5 الأدوار والمسؤوليات داخل جامعة تبوك

على جميع الجهات في جامعة تبوك تكليف لجان داخلية تتولى مسؤولية أداء الالتزامات المسندة لكل دورٍ من الأدوار الوظيفية المرتبطة بعملية تصنيف البيانات وشروط حمايتها على النحو المنصوص عليه أدناه:

- **لجنة حوكمة البيانات الداخلية للجهة:** لجنة مسؤولة عن البيانات التي تجمعها الجهة في جامعة تبوك أو تحتفظ بها، يفضل أن يكون أعضاء اللجنة من ذوي الخبرة، وتكون من مهام اللجنة:

1. تجميع البيانات: حصر الوثائق والبيانات التي تتوفر لدى الجهة والإدارات التابعة لها وفق (نموذج أ) و(نموذج ب).
2. **تصنيف البيانات:** تصنيف البيانات التي تجمعها الجهة في جامعة تبوك وفق (نموذج أ) و(نموذج ب).

3. **تجميع البيانات بعد التصنيف:** حصر البيانات بعد التصنيف ومراجعتها والتأكد من تصنيف (البيانات المجمعة من مصادرها المتعددة داخل الجهة) على أعلى مستويات التصنيف المستخدمة في تصنيف أي بيانات بشكل فردي.

4. **تنسيق تصنيف البيانات:** التأكد من أن البيانات المتبادلة بين الإدارات أو الجهات في الجامعة مصنفة ومحمية بصورة متسقة.

5. **الامتثال لسياسات جامعة تبوك لتصنيف البيانات (بالتنسيق مع إدارة الأمن السيبراني ووحدة حوكمة البيانات):** التأكد من أن البيانات محمية وفقاً للضوابط المحددة.

- **مراجع تصنيف البيانات (ممثل إدارة الأمن السيبراني):** أحد منسوبي إدارة الأمن السيبراني يقوم بمراجعة واعتماد مستويات تصنيف البيانات التي تحددها الجهة.

- **مختص بيانات الأعمال (عمادة تقنية المعلومات):** يكون مختص بيانات الأعمال من أعضاء إدارة الأمن السيبراني أو عمادة تقنية المعلومات أو كليهما ويتحمل مسؤولية حماية البيانات عن طريق تطبيق الضوابط المعتمدة المحددة في قسم "ضوابط تصنيف البيانات" بالإضافة إلى ذلك، الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزن البيانات ودعمها، وتتألف مسؤوليات مختص بيانات الأعمال من:

1. **التحكم في الوصول:** التأكد من تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقًا لمستويات تصنيف البيانات التي يحددها ممثل بيانات الأعمال في جامعة تبوك.

2. **تقارير المراجعة:** إرسال تقرير سنوي إلى مسؤولي البيانات في جامعة تبوك يتناول توافر البيانات المصنفة وسلامتها وسريتها.

3. **النسخ الاحتياطي للبيانات:** إجراء نسخ احتياطية منتظمة للبيانات.

4. **التحقق من صحة البيانات:** التحقق من صحة البيانات بشكل دوري.

5. **استعادة البيانات:** استعادة البيانات من وسائط النسخ الاحتياطي.

6. **نشاط المراقبة:** مراقبة الأنشطة التي تتم على البيانات وتسجيلها، بما في ذلك البيانات المتعلقة بالشخص الذي يصل إلى هذه البيانات.

7. **الامتثال لتصنيف البيانات (بالاشتراك مع مسؤولي البيانات)**: التأكد من تصنيف بيانات جامعة تبوك وحمايتها بعد العملية الموضحة في هذه السياسة ووفقاً للضوابط المحددة.

**مستخدم البيانات:** الموظف في جامعة تبوك الذي يتعامل مع البيانات أو يصل إليها أو يستخدمها أو يحدّثها بغرض أداء مهمة تخولها له الجهة، ويستغل المستخدمون البيانات بطريقة تتوافق مع الغرض المحدد، وكذلك الامتثال لهذه السياسة وجميع السياسات المتعلقة باستخدام البيانات في جامعة تبوك، ويُكلف المسؤول الأول في الجهة من يراه من ذوي الاختصاص لأداء هذه الأدوار.

**مدير النظام**: كل شخص مخول بإدارة أحد أنظمة الجامعة الالكترونية، و هو مسؤول عن إضافة مستخدمين لبيانات النظام حسب ما تفتضيه طبيعة عملهم.

[SDAIA, 2021]

## 6. المرجعيات

- ISO/IEC 27001:2013, A.8.2
- ECC-1:2018, 2-1
- ECC-1:2018, 2-7
- الهيئة السعودية للبيانات والذكاء الصناعي [SDAIA, 2021]

## 7. الالتزام

- يجب أن تتوافق سياسة تصنيف الأصول وترميزها مع الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (ECC:1-2018) ومع جميع متطلبات معيار الأيزو العالمي لأمن المعلومات (ISO/IEC 27001:2013).
- ينبغي الالتزام بسياسة تصنيف الأصول وترميزها من قِبَل جميع المستخدمين والموظفين والأطراف المعنية ذات العلاقة، ويجب على جميع مدراء الإدارات والأقسام التَأَكُد من الالتزام المُستَمر بتطبيقها.

- يَنبغي مُراجعة الالتزام بتَطبيق السياسة دَورياً بواسطة إدارة الأمن السيبراني, كما يَجِب على الإدارة العليا اتخاذ كافة الإجراءات التصحيحية اللازمة حال حدوث أي انتهاك للسياسة. ويجب أنَّ تَتكافأ حِدّة الإجراءات التأديبية مع حجم الانتهاك أو جَسامة الحادِث المُرتَكَب، ويَتَحَدَّدْ ذلك عَقب الانتهاء من التحقيقات اللازمة والتي بِدورها قد تُسفِر عن التالي، على سبيل المثال لا الحصر:
  - فَقْدْ امتيازات الوصول إلى الأصول المعلوماتية والتقنية.
  - تطبيق بعض العقوبات يكون حَسبما تَراه الإدارة العليا مناسباً وفق الأنظمة والتعليمات والتشريعات من الهيئة الوطنية للأمن السيبراني والقوانين الرسمية الخاصة بالجرائم المعلوماتية.

## 8. معايير الاستثناءات

- تَهْدُف هذه الوثيقة إلى تَلبية جميع مُتطلّبات الأمن السيبراني. وبُنَاءً عليه, يَجِب تَقديم طَلَبْ رَسمِي، عند الحاجة إلى الحُصول على استثناء. ويُقَدَّم الطَلب إلى إدارة الأمن السيبراني, مع ذِكْر حيثيات طلب الاستثناء بوضوح، وعَرْض الفوائد المَرْجُوَّة من هذا الاستثناء، ليتم البَتّ فيه ومَنْح الموافقة النِهائية من قِبَلْ مدير إدارة الأمن السيبراني أو اللجنة الإشرافية للأمن السيبراني ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
- تَصِل فترة الاستثناء لمُدَّة عام واحد كَحدّ أقصى, إلَّا أنَّه يُجوز إعادة تقييم طَلَب الاستثناء وتَجدِيد المُوافقة عليه بحد أقصى ثلاث أعوام متتالية إذا اقتضَى الأَمر، ولا يَجُوز مَدّ العَمَل بالاستثناء لفترات أُخرى بعد انتهاء الثَلاث أعوام السالِف ذِكْرِهُم.

## 9. المصطلحات والتعريفات

| المصطلح | التعريف |
|---|---|
| **الأمن السيبراني** | حسب ما نص عليه تنظيم الهيئة الوطنية للأمن السيبراني، الصادر بالأمر الملكي رقم (6801) وتاريخ (1439/2/11هـ) فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك. |

| | |
|---|---|
| **NCA** | الهيئة الوطنية للأمن السيبراني. |
| **ISO** | المنظمة الدولية للمعايير (منظمة الأيزو). |
| **ECC** | الضوابط الأساسية للأمن السيبراني. |
| **الأصل** | أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة). |
| **السرية** | الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية. |
| **سلامة المعلومات** | الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات والموثوقية. |
| **التَو افُر** | ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب. |
| **حادِثة** | انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني. |
| **التَحَقُّق** | التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام |
| **صلاحية المستخدم** | خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى بعض الموارد وكذلك أمن الأصول المعلوماتية والتقنية للجهة بصفة عامة وضوابط الوصول بصفة خاصة. |
| **ضابط** | مقياس لتقييد و معالجة المخاطر. |
| **المخاطر** | المخاطر التي تَمِسّ عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المُصَرَّح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نُظم المعلومات. |
| **الثغرة** | أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يَجعَل الأمن السيبراني عُرَضَة للتهديد. |
| **هجوم** | أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها. |
| **انتهاك أمنى** | الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بقصد أو بغير بقصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح التشفير وغيرها من المعايير الأمنية السيبرانية الحرجة). |
| **تهديد** | أي ظرف أو حدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلا أحد أنظمة المعلومات عن طريق الوصول غير المُصرَّح به إلى المعلومات أو |

| | |
|---|---|
| | تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية. |
| **تصنيف البيانات والمعلومات** | تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف. يتم تعيين مستويات حساسية البيانات والمعلومات وفقاً لفئات محددة مسبقاً حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة. |
| **ترميز أو وَضْع علامة** | عرض معلومات على هيئة مُلصَقات (بتسمية وترميز محدد وقياسي) توضع على أصول الجهة (مثل: الأجهزة والتطبيقات والمستندات وغيرها) ليستدل بها لإشارة إلى بعض المعلومات المتعلقة بتصنيف الأصل وملكيته ونوعه وغيرها من المعلومات المتعلقة بإدارة الأصول. |