سياسة ضبط الدخول

	عمادة التعاملات الإلكترونية والاتصالات إدارة البوابة الالكترونية	رقم الوثيقة	رقم الإصدار	اعتماد ادارة التطوير والجودة	اعتماد العميد
			1		
	سياسات وإجراءات إدارة المخاطر وأمن المعلومات				

1- هدف الوثيقة:

تهدف هذه السياسة إلى إدارة الدخول المنطقي والمادي، بحيث يقتصر على الأشخاص المفوضين والأجهزة المصرح بها داخل جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

2- مجال التطبيق:

تنطبق هذه السياسة على جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)، وعلى كافة الأطراف الأخرى بما في ذلك الشركاء، أو الجهات التابعة لها، وعلى نظم معالجة البيانات ونظم ضبط العمليات التي تحتوي على، أو تستخدم معلومات و/أو تسهيلات تعود ملكيتها لجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

تسري هذه السياسة على كافة الموظفين/ المستخدمين الذين يعملون بصورة مباشرة أو غيرة مباشرة لدى جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)، أو الجهات التابعة لها أو أية جهة تقوم بتنفيذ عمل نيابة عنها يتضمن استخدام الأصول المعلوماتية التابعة لها.

3- تطبيق الالتزام بالسياسة :

يعتبر التقيُّد بهذه الوثيقة إلزامي، وعلى عمادة التعاملات الإلكترونية والاتصالات بجامعة الملك سعود، متابعة مدى الالتزام بها ضمن إداراتهم. ويكون الالتزام ببيان السياسة العامة خاضعا للمراجعة الدورية من قبل إدارة المخاطر وأمن المعلومات، ويسفر أي انتهاك لهذه السياسة عن قيام اللجنة التوجيهية لنظام إدارة أمن المعلومات باتخاذ إجراءات تأديبية.

يتلاءم مستوى الإجراءات التأديبية المطبقة مع مستوى المخالفة الذي تتوصل إليه التحقيقات. وتتضمن هذه الإجراءات التأديبية، عقوبات قد تنطوي على إنهاء خدمة الموظف، أو أية عقوبات أخرى وفقا لتقديرات عمادة التعاملات الإلكترونية والاتصالات وإدارة الموارد البشرية.

4- معايير الاستثناء من السياسة:

تسلط هذا السياسة الضوء على متطلبات أمن المعلومات. وفيما لو دعت الحاجة للحصول على استثناء من هذه السياسة، يمكن تقديم طلب رسمي إلى اللجنة التوجيهية لنظام إدارة أمن المعلومات، مع توضيح مسوغات الاستثناء، والمزايا التي قد تنجم عن منحه.

يبلغ الحد الأقصى للاستثناء من السياسة مدة عام واحد، وفيما لو اقتضى الأمر، يمكن أن إعادة النظر بالاستثناء واعتماده مرة أخرى لثلاث فترات متعاقبة كحد أقصى. على أن لا يتجاوز الاستثناء من السياسة مدة 3 فترات متعاقبة.

5- السياسات ذات العلاقة :

- سياسة الالتزام.
- سياسة أمن المعلومات.
- سياسة إدارة الاتصالات والعمليات.

- سياسة أمن الموارد البشرية.
- سياسة الأمن المادي والبيئي.

6- مالك الوثيقة:

إدارة نظم إدارة أمن المعلومات

7- إدارة السياسة :

تقتضي التطورات التقنيّة والتغييرات على متطلبات العمل، إجراء مراجعات دورية للسياسات .ومن هذا المنطلق، فإن هذه السياسة قد تخضع للتعديل بهدف تطبيق التغييرات التي تمت، أو وضع متطلبات جديدة أو محسنة.
يجب إبلاغ مسئول أمن المعلومات فورا، بأي قصور يتم اكتشافه في هذه السياسة .علما بأن إجراء التغييرات على هذه الوثيقة يتطلب موافقة اللجنة التوجيهية لنظام إدارة المخاطر وأمن المعلومات. ينبغي الاحتفاظ بسجل حديث للتغييرات، وان يتم تحديثه فور حدوث أي تغيير.

8- بيان السياسة :

يتعين بيان قواعد وحقوق الدخول الخاصة بكل مستخدم أو مجموعة من المستخدمين بوضوح. وينبغي أخذ كلا النوعين من الدخول، المنطقي والمادي، بعين الاعتبار معا، وذلك بهدف تطبيق الأمن بالشكل الأمثل.

8.1. متطلبات العمل الخاصة بالدخول إلى المعلومات

8.1.1. يجب ضبط عملية الدخول للمعلومات بناءً على متطلبات العمل، والمتطلبات الأمنية، وقواعد ضبط الدخول الخاصة بكل نظام من نظم أمن المعلومات. وينبغي لهذه القواعد أن تراعي ما يلي:

- المتطلبات الأمنية لتطبيق / تطبيقات العمل.
- وجود حاجة محددة ترتبط بالعمل تقتضي منح المستخدم حق الدخول إلى المعلومات أو إجراءات العمل (مبدأ "الحاجة إلى المعرفة").
- حظر كافة أشكال الدخول ما لم تصدر موافقة محددة على ذلك بموجب أحكام هذه السياسة.
- الالتزامات القانونية و/ أو التعاقدية لتقييد وحماية عمليات الدخول إلى نظم المعلومات.

8.1.2. يمنح المقاولون أو الاستشاريون أو موظفو الطرف الثالث حق الدخول إلى معلومات العمل في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) بعد إبرام اتفاقية تعاقدية. على أن تتضمن هذه الاتفاقية ما يلي، وذلك على سبيل المثال لا الحصر:

- الأحكام والشروط الخاصة بالدخول المصرح به.
- المسئوليات الأمنية للمقاولين، والاستشاريين أو الموظفين التابعين للمورّد.
- موافقة المقاولين والاستشاريين أو موظفي الطرف الثالث على الالتزام بسياسات أمن المعلومات في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

8.2. إدارة حسابات المستخدمين

8.2.1. تتولى جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) وضع إجراءات رسمية لضبط الدخول، بحيث تتضمن هذه الإجراءات خطوات واضحة بخصوص طلب، وإنشاء، وتعديل، وتعليق وإلغاء حسابات المستخدمين.

8.2.2. يتولى مالك الأصل مسئولية التفويض بمنح الدخول للمستخدمين، وإجراء التعديلات على حقوق الدخول الحالية الخاصة بهم، وإلغاء هذه الحقوق، على أن يؤخذ ما يلي بعين الاعتبار:

- منح أقل الامتيازات (مبدأ "الحاجة إلى المعرفة").
- الفصل بين المهام والمسئوليات.
- مستوى الدخول المطلوب.

8.2.3. يُزود كل مستخدم ببيانات دخول توضح هويته، على أن تتطلب هذه البيانات ما لا يقل عن عامل واحد من عوامل المصادقة (مثل كلمة المرور، رقم رمز المطابقة Token، أجهزة التعرف من خلال الخصائص الحيوية Biometric).

8.3. التفويض بالدخول والامتيازات

8.3.1. يجب العمل على تحديد وتوثيق كافة المستخدمين المفوضين الذين يدخلون إلى الأصول المعلوماتية التابعة لجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات). ويتم متابعة وتسجيل إجراءات التفويض وفقاً لما يلي:

- تاريخ منح التفويض.
- تحديد إجراءات الموافقة على منح التفويض.
- توفير وصف للامتيازات الممنوحة.
- بيان الأسباب التي دعت إلى منح التفويض.

8.3.2. الالتزام بمبدأ الفصل بين المهام والمسئوليات، ومبدأ أقل الامتيازات عند منح صلاحية الدخول للمستخدمين في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

8.4. إدارة كلمات المرور الخاصة بالمستخدمين

8.4.1. في حالة وجود أي شك بانكشاف كلمة المرور، يجب العمل فوراً على تغيرها، وإبلاغ إدارة رعاية العملاء فورا بذلك.

8.4.2. تتولى عمادة التعاملات الإلكترونية والاتصالات تغيير كافة أسماء المستخدمين وكلمات المرور الافتراضية قبل بدء تشغيل نظام أمن المعلومات.

8.4.3. يتعيّن على المستخدمين وإداري النظام مراعاة ما يلي عند اختيار كلمة المرور:

- أن لا يقل الحد الأدنى لطول كلمة المرور عن 8 خانات.
- تتكون كلمة المرور من مزيج مما يلي:
  - ✓ ما لا يقل عن حرف هجائي واحد كبير (Uppercase)[A-Z]

- ✓ ما لا يقل عن حرف هجائي واحد صغير (Lowercase)[a-z]
- ✓ ما لا يقل عن حرف واحد من الحروف الخاصة (مثل @، %)
- ✓ ما لا يقل عن عدد واحد (0-9)

- أن لا يتم وضع كلمة المرور بناءً على معلومات شخصية، كأسماء العائلة أو ما إلى ذلك.
- أن لا تكون كلمة المرور قابلة للتخمين أو كلمة من القاموس.
- لا يسمح بترك كلمة المرور خالية.
- على المستخدمين تغيير كلمة المرور عند تسجيل الدخول لأول مرة إلى أي نظام.
- يتم تعطيل حساب المستخدم بعد 3 محاولات فاشلة لتسجيل الدخول.
- ينبغي فرض عملية تغيير كلمة المرور (من قبل نظام التشغيل أو التطبيق) كل 42 يوما على الأقل. ويجب أن لا تكون كلمة المرور الجديدة مماثلة لأي من كلمات المرور الثمانية القديمة (كلمات المرور السابقة).
- تستخدم كلمة المرور المبدئية لمرة واحدة فقط
- تحفظ كلمة المرور ويتم تداولها بصورة محمية (مشفرة أو مخفية).

8.5 مراجعة حقوق دخول المستخدمين

8.5.1 يتولى مالك الأصل، بالتعاون مع يقوم مسئول أمن المعلومات والإدارات المعنية مراجعة حقوق دخول المستخدمين بما لا يقل عن مرة واحدة في العام.

8.5.2 فور اكتشاف أي سوء تصرف في حقوق الدخول الممنوحة، يقوم مسئول أمن المعلومات يجب أن توصي مدير دائرة بتقييد هذه الحقوق.

8.6 ضبط كلمة المرور

8.6.1 يحظر على المستخدمين إدخال كلمات المرور في رسائل البريد الإلكتروني أو المراسلات الإلكترونية.

8.6.2 يحظر على المستخدمين توزيع كلمات المرور الخاصة بهم على المستخدمين الآخرين، وبالتالي فإنهم يتحملون المسئولية الكاملة عن أية أنشطة لها صلة بحقوق الدخول الممنوحة لهم.

8.6.3 يحظر على المستخدمين التقاط أو الحصول على كلمات المرور، أو مفاتيح فك التشفير، أو أية آلية أخرى من آليات التحكم بالدخول من شأنها السماح بالدخول بدون تفويض.

8.7 حماية أجهزة المستخدمين المتروكة دون إشراف

8.7.1 يجب على كافة المستخدمين تشغيل شاشات التوقف المزودة بكلمات مرور على كافة الأصول المعلوماتية (مثل الحواسيب الشخصية، والحواسيب النقالة، والخوادم) للحيلولة دون عمليات الدخول غير المصرح بها. وينبغي إعداد المؤقِّت لتشغيل شاشة التوقف بعد مرور 10 دقائق من عدم استخدام الجهاز.

8.7.2 على كافة المستخدمين، وعند الانتهاء من أداء أعمالهم، إنهاء كافة فترات الاتصال النشط بالشبكة (Active Sessions).

8.7.3 على كافة المستخدمين إغلاق الأجهزة الخاصة بكل منهم قبل مغادرة المكتب.

8.8 أمن المكتب النظيف والشاشة الخالية

8.8.1 كحد أدنى، ينبغي اتباع الإرشادات التالية وتطبيقها من قبل كافة المستخدمين لتعزيز سياسة المكتب النظيف والشاشة الخالية في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات):

- عند عدم استخدام الأوراق والوسائط التي تحتوي على معلومات، وخصوصاً فيما بعد ساعات الدوام الرسمي، ينبغي حفظها في خزانات مناسبة ومقفلة و/أو أي نوع آخر من الأثاث الذي يوفر الحماية.
- ينبغي حفظ الوثائق الحساسة أو الحيوية المرتبطة بالعمل في مكان بعيد ومقفل عند عدم الحاجة إليها (ويفضل أن يكون ذلك ضمن خزنة أو خِزانة مقاومة للحريق)، أو عندما تخلو المكاتب من الموظفين.
- يتعين عدم ترك الحواسيب الشخصية، والحواسيب المربوطة (Terminals)، والطابعات في وضعية تسجيل الدخول (Logged on) في حالة تركها بدون إشراف، وينبغي حمايتها من خلال شاشة توقف مزودة بكلمة مرور.
- يجب إقفال أجهزة تصوير الوثائق والفاكس (أو حمايتها من الدخول غير المصرح به بطريقة أو بأخرى) بعد ساعات الدوام الرسمي.
- عند طباعة أي معلومات سرية، يتوجب على الفور إزالة الوثائق ذات العلاقة من الطابعات.

8.8.2 على مدير نظام إدارة أمن المعلومات تعميم سياسة المكتب النظيف والشاشة الخالية على الموظفين الذي كل في مجال عمله، مع المراقبة الدورية لأنشطتهم للتأكد من التزامهم بتلك السياسة.

8.8.3 على مسئول أمن المعلومات ضمان حضور كافة موظفي جامعة الملك سعود لدورات تدريب ملائمة تتعلق بالتوعية الأمنية، بحيث يتطرق هذا التدريب إلى سياسة المكتب النظيف والشاشة الخالية.

8.9 موارد الشبكة

8.9.1 يتم تفويض وضبط الدخول إلى الشبكة وخدماتها وفقاً لمتطلبات العمل والأمن وقواعد الدخول المحددة لكل شبكة، على أن تراعي هذه القواعد ما يلي:

- المتطلبات الأمنية للشبكة ولخدمة/ خدمات الشبكة.
- وجود حاجة محددة، ذات صلة بالعمل، لدى المستخدم للدخول إلى المعلومات أو عمليات العمل (وفقاً لمبدأ الحاجة للمعرفة).
- التصنيف الأمني للمستخدم والتصنيف الأمني للشبكة.
- الالتزامات القانونية و/ أو التعاقدية لتقييد أو حماية الدخول إلى نظم المعلومات.

8.10 المصادقة في حالة الدخول عن بُعد

8.10.1 يجب اقتصار عملية دخول المستخدمين عن بُعد إلى شبكات جامعة الملك سعود على أولئك المستخدمين الحاصلين على تفويض بذلك، مع مراعاة الالتزام بالأساليب المناسبة للمصادقة على المستخدم.

8.11. المصادقة على الدخول على أجهزة ومعدّات الشبكة

8.11.1. كجزء من متطلبات سجل الأصول العام، يتعين على عمادة التعاملات الإلكترونية والاتصالات، تحديد جميع معدات الشبكة من خلال أسماء فردية، والاحتفاظ بسجل بجميع أجهزة ومعدات الشبكة بحيث يبين مكان تواجدها والغرض منها.

8.11.2. تتكون مخططات الشبكة مما يلي، وذلك على سبيل المثال لا الحصر:

- كافة معدات وأجهزة الشبكة بالإضافة إلى عناوين بروتوكول الإنترنت (IP) الخاصة بها.
- جميع وصلات الاتصال (الرئيسية والاحتياطية) بالإضافة إلى عرض النطاق الخاص بها ونوع البيانات التي يتم استخدام الخط من أجلها (صوت / بيانات).
- آلية فعالة لضبط النُسخ.

8.11.3. يتعين الاحتفاظ بمخططات حديثة للشبكة. ويتوجب على عمادة التعاملات الإلكترونية والاتصالات إجراء مراجعات دورية لضمان تحديث مخططات الشبكة بما يعكس البنية الحالية للشبكة. كما يجب تحديث مخططات الشبكة عندما تكون هناك تغييرات على بنية الشبكة.

8.12. حماية وإدامة الدخول عن بُعد

8.12.1. يقتصر استخدام أدوات تشخيص الشبكة والأدوات الأمنية على الموظفين المعينين لهذا الغرض، ووفقاً للمسؤوليات المتعلقة بالوظائف التي يتولونها.

8.12.2. فيما يختص بأية وصلة إدارية تصرح باستخدامها جامعة الملك سعود، يراعي اللجوء إلى استخدام أساليب مُحْكمة للمصادقة (على سبيل المثال مصادقة مزدوجة)، وطرق التشفير ذات الصلة (على سبيل المثال، بروتوكول حماية المراسلات عبر الشبكة SSH ، أو طبقة المنافذ الآمنةSSL ، أو الشبكة الافتراضية الخاصة VPN).

8.13. تقسيم الشبكة

8.13.1. يتعين تقسيم شبكة نظم معلومات جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) إلى قطاعات، ومناطق، ومجالات منطقية وفقاً للمعايير التالية، والتي نوردها على سبيل المثال لا الحصر:

- متطلبات الدخول (مثل المستخدمين، تقنية المعلومات، الإدارة).
- تكلفة استخدام التقنية الملائمة، والآثار المترتبة على الأداء.
- قيمة وتصنيف المعلومات المخزنة أو التي يتم معالجتها في الشبكة (حرجة، حساسة).
- مستوى الثقة (مثال: موثوق، إنترنت، منطقة مجردة DMZ).
- طبيعة العمل (مثل :خدمات، دعم).

8.13.2. يتعين فصل الشبكة الداخلية عن الشبكة الخارجية باستخدام ضوابط محيطية أمنية مختلفة لكل شبكة من الشبكات.

8.14. التحكّم بوصلات الشبكة

تنحصر قدرة المستخدمين على الربط من خلال بوابات الشبكة، حيث تعمل هذه البوابات على تنقيح الحركة على الشبكة من خلال جداول أو قواعد محددة مسبقاً. ويتضمن ذلك ما يلي، على سبيل المثال لا الحصر:

- تبادل الرسائل (كالبريد الإلكتروني).

- نقل الملفات.
- الدخول التفاعلي.
- الدخول إلى التطبيقات.

8.15. ضبط تدفق المعلومات

8.15.1. يتعين على عمادة التعاملات الإلكترونية والاتصالات تفويض الحركة على الشبكة بناءً على متطلبات اتصالات العمل، والتنسيق مع المسئولين عن إجراءات العمل.

8.15.2. يتعين على عمادة التعاملات الإلكترونية والاتصالات تطبيق آليات لضبط التوجيه (Routing) لتقييد تدفق المعلومات بحيث ينحصر في المسارات المخصصة للشبكة.

8.15.3. يتعين على إدارة جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات). ضمان توفير وتنفيذ إدارة ملائمة وإشراف فني على هيكل محيط الأمن (كالجدران النارية) والتهيئة الحالية. هذا وسيتم تغطية ما يلي، وذلك على سبيل المثال لا الحصر:

- توثيق ومراجعة القواعد المتعلقة بالمحيط الأمني على أساس منتظم.
- توثيق التعديلات على التهيئة والحصول على موافقة الإدارة.
- الحصول على موافقة الإدارة قبيل تطبيق أية تعديلات على قواعد المحيط الأمني.
- بذل عناية كافية عند تطبيق التعديلات على قواعد المحيط الأمني لضمان أقل قدر من التشويش على بيئة جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

8.16. الدخول الآمن على نُظم التشغيل

8.16.1. ينبغي للنظام أن يعمل على تقييد عدد مرات محاولات تسجيل الدخول الفاشلة المسموح بها مع مراعاة ما يلي:

- تسجيل المحاولات الفاشلة والناجحة على حد سواء.
- فرض فترة انتظار زمنية قبل السماح بمواصلة أو رفض محاولات الدخول دون توفر تفويض محدد.
- فصل وصلة الربط بالبيانات.
- توجيه رسالة تحذير إلى وحدة التحكم (Console) الخاصة بالنظام، استنفاذ الحد الأقصى من محاولات الدخول الفاشلة.

8.16.2. على مسئولي النظام مراجعة كافة محاولات الدخول الفاشلة بشكل منتظم.

8.16.3. ينبغي أن يعمل النظام على عرض ملاحظة عامة تدل على أنه يحظر الدخول إلى الحاسوب إلا من قبل المستخدمين الحاصلين على تفويض بذلك.

8.16.4. يتعين أن تعمل إجراءات تسجيل الدخول الخاصة بأي نظام على عرض أقل قدر من المعلومات حول النظام والغرض من استخدامه.

8.17. التحقق من هوية المستخدم والمصادقة عليه

8.17.1. يتعين على النظام المصادقة على معلومات تسجيل الدخول بعد استكمال إدخال كافة البيانات. وفي حالة ظهور ما يدل على وقوع خطأ، ينبغي أن لا يعمل النظام على بيان أية جزئية من البيانات كانت خاطئة وأية جزئية كانت صحيحة.

8.17.2. يتعين على جامعة الملك سعود (الرسائل وإدارة الهوية) التعرف على الهوية/ المصادقة بخصوص كافة المستخدمين بصورة فريدة قبل منحهم الدخول إلى النظام.

8.18. ضبط البرامج الخدمية

8.18.1. يكون الدخول إلى برامج النظام محدوداً ويخضع للسيطرة.

8.18.2. يتوجب إزالة كافة البرامج الخدمية (System Utilities) والبرامج غير الضرورية.

8.19. التحكم بجلسة الاتصال بالشبكة

8.19.1. يتعين على النظام أثناء إجراءات تسجيل الدخول، العمل على تقييد الحدين الأدنى والأعلى للزمن المسموح به. وعند تجاوز هذين الحدين يتم إنهاء عملية تسجيل الدخول.

8.20. التحكم بزمن الاتصال بالشبكة

8.20.1. حيثما أمكن، يتعين أن يكون لكافة نظم المعلومات الحيوية زمن محدد للدخول والربط.

8.21. ضبط الدخول إلى نظم التطبيق

8.21.1. يجب وضع ضوابط بهدف ضبط المخرجات من نظم التطبيقات التي تتعامل مع المعلومات الحساسة، بحيث لا يتم إرسال هذه المخرجات إلا إلى الشاشات الطرفية والمواقع الحاصلة على تفويض.

8.22. عزل نظم التطبيق الحساسة

8.22.1. يجب تنفيذ عملية عزل مادية (فعلية) و/أو منطقية للنظم ذات الطبيعة الحساسة.

8.22.2. حيثما أمكن، يجب تشغيل التطبيقات الحساسة التي تتعامل مع البيانات الحساسة على أنظمة تشغيل مخصصة.

8.22.3. عند حاجة النظام ذي الطبيعة الحساسة للعمل في بيئة مشتركة، فإنه يتوجب على مالك التطبيق تحديد وقبول المخاطر المرتبطة بالموارد المشتركة.

8.22.4. يجب تهيئة التطبيقات لتعمل على تشغيل خدمات محدودة فقط، وذلك طبقاً لمتطلبات العمل في الجامعة.

8.23. ضبط أنشطة العمل عن بُعد

8.23.1. ينبغي الحصول على موافقة رسمية، وتوفير كافة الضوابط الأمنية ذات العلاقة قبل التفويض بأنشطة العمل عن بُعد.

8.23.2. ينبغي عدم استخدام الحواسيب النقالة أو الحواسيب الشخصية المنزلية في أنشطة العمل دون الحصول على التفويض الصريح من الإدارة.

8.23.3. عند انتهاء أنشطة العمل عن بُعد، يتوجب العمل فوراً على إلغاء التفويض، وحقوق الدخول، وإعادة الأجهزة.

8.23.4. يجب الاحتفاظ بسجل دقيق وحديث بحيث يحتوي على كافة الأنشطة المتعلقة بالعمل عن بُعد.

8.23.5. لا تسمح جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) باستخدام سوى الأجهزة التابعة للجامعة في أنشطة العمل عن بُعد، والربط عن بُعد بالشبكة الخاصة بالجامعة. ويتعين مراعاة الترتيبات الأمنية التالية من قبل مالك الأصل:

- ضمان توفر الأمن المادي للأجهزة الأمنية وحمايتها من السرقة/ الضياع.
- ضمان تشفير الأجهزة.
- استخدام برنامج ملائم للحماية من البرامج الضارة، وضوابط أمنية للأجهزة (كأجهزة الحماية من الفيروسات، والجدران النارية الشخصية).
- الربط مع شبكة جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) باستخدام أسلوب الأنفاق الأمنة (مثل، طبقة المنافذ الآمنةSSL ، الشبكة الافتراضية الخاصة VPN).
- تطبيق آليات مناسبة للمصادقة / للتفويض.
- حفظ نسخ احتياطية من كافة المعلومات الحساسة ذات الصلة.