مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة إدارة الوصول المنطقي			
النسخة:	١,٠			
التصنيف:	◉ عامة	○ سرية	○ سرية عالية	○ سرية للغاية
الحالة:	معتمده	**النوع :**	وثيقة	
تاريخ الإصدار:	٢٠١٥/٠٦/٢٤			
تاريخ المراجعة:	٢٠١٥/٠٦/٢٤			

النسخة رقم	التاريخ	إعداد ومراجعة	الملاحظات
١,٠	٢٠١٥/٠٦/٢٤	الإدارة العامة لتقنية المعلومات (قسم أمن المعلومات)	النسخة الأولى من الوثيقة

الموظف المختص

النسخة رقم	التاريخ	المختص	الملاحظات
١,٠	٢٠١٥/٠٦/٢٤	محمد الشهري	تم المراجعة

الإعتماد

النسخة رقم	التاريخ	المعتمد/ المعتمدين	الملاحظات
١,٠	٢٠١٥/٠٧/٠٨	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد	

جدول المحتويات

١. تعريف هيكلة السياسة

تشتمل وثيقة السياسة على العناصر التالية:

- **الهدف:** وصف مختصر لأغراض وأهداف السياسة.
- **نطاق العمل:** تحدد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.
- **الإمتثال والتنفيذ:** تحدد تبعات ونتائج أية مخالفة لهذه الساسة.
- **السياسات:** يشتمل هذا القسم على وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.

٢. الهدف

الغرض من هذه السياسة هو التحكم بالوصول المنطقي إلى أنظمة معلومات جامعة الملك خالد، بما يكفل دقة وسرية وتوفر المعلومات.

٣. نطاق العمل

تطبق هذه السياسة على جميع الموظفين، والموردين، وشركاء العمل، والموظفين المتعاقدين، والوحدات الوظيفية لدى جامعة الملك خالد سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم. كما تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٤. الإمتثال و التنفيذ

في حالة مخالفة أي موظف أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لدى جامعة الملك خالد لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر- نظام العمل والعمال، ونظام مكافحة الجرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٥. **السياسات** :

- **التحكم بالوصول**

- يجب أن يسمح لجميع المستخدمين لدى الجامعة بالوصول إلى أنظمة المعلومات والعمليات اللازمة لتأدية مهام أعمالهم فقط.
- يجب استخدام (إجراءات استحداث مجموعات المستخدمين) لضبط إعدادات الوصول لأنظمة المعلومات عند تطبيق و إعداد الأنظمة و ذلك باستخدام خاصية مجموعات المستخدمين والتي تحدد امتيازات الوصول لكل مجموعه. و يجب أن لا يتم تعيين امتيازات وصول مستقلة للمستخدمين الأفراد، وإنما يتم منحهم إمكانية الوصول من خلال عضويتهم في مجموعات المستخدمين المحددة مسبقاً.
- يجب التحكم بالوصول إلى أنظمة المعلومات لدى الجامعة باستخدام إجراءات تسجيل دخول المستخدمين فقط. ويجب عدم منح أي مستخدم إمكانية الوصول قبل استكمال كافة إجراءات تسجيل دخول المستخدم.
- على كل مستخدم من مستخدمي أنظمة المعلومات الحصول على تفويض من المسئول عن نظام المعلومات كي يتسنى له الدخول إلى أنظمة معلومات الجامعة.
- يسمح الوصول إلى نظم المعلومات وتفعيل حسابات المستخدمين للموظفين والمتعاقدين والاستشاريين والموظفين المؤقتين، أو أفراد الموردين؛ فقط عندما يكون الفرد يقدم خدمة للجامعة. (راجع القسم الفرعي "وصول الأطراف الثالثة إلى أنظمة معلومات الجامعة" في هذه السياسة لضوابط إضافية يجب اتباعها عند تقديم الوصول إلى أطراف ثالثة).

- **اسم المستخدم وكلمة المرور**

- يجب أن يتم تخزين والتعامل مع وتوزيع كافة أسماء المستخدمين وكلمات المرور إلى الأنظمة بشكل آمن.
- يجب أن يكون لكل مستخدم من مستخدمي أي نظام معلوماتي اسم مستخدم فريد وكلمة مرور خاصة به.
- يجب عدم استخدام أسماء المستخدمين المشتركة و الأسماء الشائعة و العامة.
- لا يسمح للمستخدم بمشاركة اسم المستخدم وكلمة المرور الخاصين به مع أشخاص آخرين تحت أي ظرف من الظروف. وعلى المستخدم أن يتحمل المسؤولية المباشرة كاملة عن كافة الأنشطة التي تتم من خلال حساب المستخدم الخاص به على أي من الأنظمة المسموح له استخدامها.
- يجب عدم إعادة إصدار نفس اسم المستخدم لمستخدمين آخرين.
- يجب أن تكون معايير تحديد اسم المستخدم متوافقة مع معايير التسمية المعيارية لدى الجامعة بما يضمن أن اسم المستخدم لا يعطي أي انطباع حول مستوى المستخدم أو امتيازاته أو حقوق الدخول التي يتمتع بها، مثل (verifier) أو (Releaser).
- ينبغي على جميع المستخدمين بمن فيهم مدراء الأنظمة الإلتزام بالأحكام والشروط المتعلقة باستخدام وإدارة كلمات المرور الخاصة بهم بما تنص عليه سياسة معايير كلمة المرور (يرجى الرجوع الى السياسات الأمنية العامة).

- يجب تحديد ميزات حجب اسم المستخدم وانتهاء صلاحية كلمة المرور بناءً على متطلبات النظام، وتصنيفه، وأهميته (كونه من الأنظمة الحرجة)، والآثار الجانبية في حال الإنتهاك.

- **إدارة امتيازات الدخول للأنظمة**

- يجب حصر جميع الحسابات ذات المزايا العالية (مثل حسابات مدراء الأنظمة أو الحسابات الأساسية (root accounts). على عدد قليل من الأشخاص المصرح لهم باستخدام هذه الحسابات. ويجب عدم تعيين أي امتيازات قبل اكتمال إجراءات التفويض المتعلقة بهذا الصدد.
- يجب عدم منح أي امتيازات لحسابات مستخدمي تقنية المعلومات كمدير نظام محلي أو بعيد أو مدير نطاق إلا في حال وجود مبرر لذلك.
- يجب إتباع مبدأ الفصل في الامتيازات عند تعيين امتيازات الوصول لأنظمة المعلومات لمستخدمي تقنية المعلومات.
- يجب عدم منح موظفي عمليات تقنية المعلومات إمكانية الوصول إلى بيئة تطوير الأنظمة.
- يجب عدم منح موظفي تطوير الأنظمة إمكانية الوصول إلى بيئة عمليات تقنية المعلومات.
- عندما يتعذر الفصل في المهام أو عندما لا يكون ذلك ممكناً من الناحية العملية، يجب أن تتضمن العملية ضوابط تعويضية مثل مراقبة الأنشطة، إبقاء ومراجعة سجل الفحص والمراجعة والإشراف الإداري.

- **تغيير وصول المستخدم**

- يجب التأكد من أنه يتم الإلغاء الفوري لجميع حسابات المستخدمين بمجرد إنهاء خدمتهم أو انتهاء عقودهم، أو تغيير وظائفهم، أو عندما لم يعد لمستخدم معين حاجة عملية للوصول إلى نظام المعلومات.
- في حالة انتهاء أو إنهاء عقد الموظف أو انتقاله، يجب على إدارة الموارد البشرية أو الإدارات ذات الصلة أن تقوم فوراً بإشعار الإدارة العامة لتقنية المعلومات من خلال البريد الإلكتروني وتزويدهم بتفاصيل قرار تغيير الوظيفة أو الانتقال وتاريخ النفاذ.

- **مراجعة حقوق الوصول للمستخدم**

- يجب أن تقوم الإدراة العامة لتقنية المعلومات بإجراء مراجعة دورية تتعلق بالمخاطر المترتبة عن حقوق وصول المستخدمين للأنظمة.
- يجب أن تتأكد الإدارة العامة لتقنية المعلومات من أن جميع حقوق وصول المستخدمين قد تمت مراجعتها من قبل المسئولين عن الأنظمة المعلوماتية وفقاً لإجراءات مراجعة حقوق وصول المستخدمين للتأكد من:
  - مطابقتها لأوصاف وظائف المستخدمين.
  - الاستمرار في الحفاظ على متطلبات الفصل بين المهام.
  - الاستمرار في إتباع مبدأ "الحاجة إلى المعرفة".

- ينبغي على الإدارة العامة لتقنية المعلومات إجراء مراجعات دورية للنظام لاكتشاف الحسابات غير المستخدمة، حيث يتعين تعطيل تلك الحسابات ومن ثم إزالتها من النظام.
- عند اكتشاف أي سوء استخدام لحقوق الوصول المميزة، فإن على الإدارة العامة لتقنية المعلومات تقييد تلك الامتيازات وإشعار إدارة الموارد البشرية أو الإدارات ذات الصلة والمسؤول عن أنظمة المعلومات لاتخاذ الإجراء اللازم حيال ذلك.

- **سياسة المكتب الخالي والشاشة الخالية**

- يجب عدم ترك أجهزة الحاسوب المحولة وأجهزة سطح المكتب ووحدات الحاسوب الطرفية والطابعات مفتوحة في حالة عدم التواجد بجوارها، وإنما يجب تحصينها بشاشات محمية بكلمات مرور.
- يجب تحصين أجهزة تصوير المستندات وأجهزة الفاكس بكلمات مرور.
- يجب رفع المعلومات الحساسة والمصنفة عند طباعتها فوراً من الطابعات.

- **مرافق معالجة المعلومات**

- يجب التفويض رسمياً من قبل الإدارات ذات العلاقة ومشرف الإدارة العامة لتقنية المعلومات قبل استخدام أي من أنظمة المعلومات المستخدمة لاستقبال وتخزين ومعالجة البيانات لدى الجامعة.
- لا يسمح لأي مستخدم باستعمال أي أنظمة معلومات شخصية أو مملوكة شخصيا، مثل الحواسيب المحمولة وأجهزة الحاسب الآلي المنزلية والأقراص الصلبة الخارجية وأدوات التخزين الخارجية (flash disks) والأجهزة اليدوية دون موافقة الإدارة العامة لتقنية المعلومات.
- يجب أن تتوافق أنظمة المعلومات المستخدمة لشراء أو معالجة البيانات لدى الجامعة مع معايير أمن المعلومات لدى الجامعة حسبما تم تطويره بشكل عام أو خصيصاً للنظام.

- **وصول الأطراف الثالثة إلى أنظمة معلومات الجامعة**

- على الإدارة العامة لتقنية المعلومات إجراء تقييم لتحديد المخاطر المحتملة لأنظمة المعلومات لدى الجامعة، والناشئة عن وصول أطراف أخرى إليها.
- يجب الأخذ بعين الاعتبار أن يتضمن التقييم المذكور المعايير التالية:
  - نوع ومستوى الوصول الذي سيتم منحه للطرف الآخر.
  - تصنيف مخاطر أنظمة المعلومات التي سيتم السماح بالوصول إليها.
  - الأسباب التي على أساسها يتم منح الوصول لأنظمة المعلومات.
  - المعلومات المرجعية عن الطرف الآخر.
  - توفر وفاعلية الضوابط الواجب تطبيقها لتنظيم ومراقبة وصول الطرف الآخر.
- يتم منح إمكانية وصول الطرف الآخر لأنظمة المعلومات لدى الجامعة بناءً على عقد رسمي بين الجامعة و الطرف المذكور.

- يجب أن يتضمن العقد الشروط التالية كحد أدنى:
  - الشروط والأحكام التي يتم منح الوصول بموجبها.
  - مستوى الأمن الطبيعي والمنطقي الذي سيقدمه (الطرف الثالث) للحفاظ على سرية وتكامل وسلامة معلومات/ بيانات الجامعة التي يتم معالجتها.
  - مسؤوليات المتعاقدين أو الاستشاريين أو الموردين.

- يجب الحصول على تصريح لوصول جميع موظفي الطرف الثالث إلى أنظمة المعلومات لدى الجامعة من قبل الإدارات المعنية. يجب أن يتضمن التصريح إيضاح مبررات الوصول وفترة الوصول المطلوبة و قائمة أنظمة المعلومات التي سيتم منح الوصول إليها والمعلومات الأخرى المرتبطة بذلك. وعلى الإدارة العامة لتقنية المعلومات مراجعة الطلب قبل تنفيذه.
- يجب أن تحديد تاريخ انتهاء إسم المستخدم للموظفين المتعاقدين والإستشاريين وجميع موظفي الطرف الثالث الآخرين مع مراعاة أن لا يتجاوز تاريخ انتهاء المشروع المتعاقد عليه.

- **الوصول عن بعد**

- يمنح الوصول عن بعد لشبكة الجامعة بإستخدام إجراءات تسجيل دخول المستخدمين.
- يمنح الوصول عن بعد على أساس الحاجة ولأغراض العمل فقط.
- تمنح الجامعة إمكانية الوصول عن بعد فقط للاحتياجات التشغيلية الضرورية وتوثق مبررات هذا الوصول ضمن إجراءات تسجيل دخول المستخدمين.
- يتم اعتماد الوصول عن بعد من قبل الإدارة العامة لتقنية المعلومات إضافة إلى الموافقات الاعتيادية.
- يجب على المستخدمين الحاصلين على إمكانية الوصول عن بعد التأكد من أن أجهزة الحاسب الآلي أو محطة العمل الشخصية أو المملوكة من قبل الجامعة، الموصولة عن بعد مع شبكة الجامعة تتصف بما يلي:
  - غير موصولة مع أية شبكة أخرى في نفس الوقت باستثناء الشبكات الشخصية الخاضعة للسيطرة الكاملة من قبل ذلك المستخدم.
  - تتضمن أحدث برامج مكافحة الفيروسات والتجسس والجدار الحماية.
- يجب أن تتحكم الجامعة بجميع حالات الوصول عن بعد عبر عدد محدود من النقاط المدارة للتحكم بالوصول.
- يتحمل المستخدم المسئولية عن أن أية تبعات أو آثار سلبية ناشئة عن إساءة استخدام الوصول.
- يجب تسجيل كافة أنشطة وصلات الدخول عن بعد بما في ذلك عنوان بروتوكول الإنترنت واسم المستخدم الخاص بالدخول.
- يجب مراقبة النشاطات المجراة عبر الحساب. في حالة عدم استخدام الحساب لمدة ثلاثة أشهر يجب إنهاؤه وإيقافه. وإذا تم طلب الوصول مرة أخرى، فعلى المستخدم أن يطلب حساباً جديداً.

- يجب أن يكون للوصول عن بعد آليات قوية للتحقق من الهوية مثل التحقق باستخدام كلمة مرور تستخدم لمرة واحدة أو مفاتيح عامة/ خاصة مع مقاطع قوية لكلمة المرور.
- يجب عدم منح الأطراف الثالثة إمكانية الوصول عن بعد إلى أنظمة معلومات الجامعة إلا إذا كان هناك مبرر عملي قوي لذلك. وإذا ما تم منح الغير إمكانية الوصول عن بعد إلى أنظمة/شبكات معلومات الجامعة، يجب مراعاة ما يلي:
  - أن يكون دخول الغير محدوداً فقط على شبكة/نظام معلومات محدد مطلوب لتأدية المسؤوليات المناطة بتلك الأطراف.
  - أن تتم مراقبة سجلات وأنشطة الوصول عن كثب من قبل الإدارة العامة لتقنية المعلومات.