# جامعة الإمام عبدالرحمن بن فيصل
# IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

## سياسة العمل عن بعد

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-37.CS. A. V2.0

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

## 1. جدول المحتويات

## 2. معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة الاتصالات وتقنية المعلومات في جامعة الإمام عبد الرحمن بن فيصل. وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة الاتصالات وتقنية المعلومات.

## 3. الرقابة على الوثيقة

### 1.3 معلومات عن الوثيقة

| العنوان | التصنيف | الإصدار | الحالة |
|---|---|---|---|
| سياسة العمل عن بعد | مقيد | V2.0 | فعال |

### 2.3 تاريخ الإعداد والتّحديث

| الإصدار | المؤلفون | تاريخ الاصدار | التغييرات |
|---|---|---|---|
| V1.0 | د. بشار الذيب | 2021/03/12 | إنشاء |
| V1.1 | د. سامر بني عواد | 2022/02/14 | مراجعة وتحديث |
| V2.0 | بهاء نوافله | 2023/12/26 | مراجعة وتحديث |
| | | | |
| | | | |

### 3.3 المراجعة والتدقيق

| تاريخ المراجعة القادمة |
|---|
| 2025/01/01 |

### 4.3 قائمة التوزيع

| الرقم | المستفيد |
|---|---|
| 1 | جميع أقسام عمادة الاتصالات وتقنية المعلومات |
| 2 | الشؤون القانونية |
| 3 | الموقع الإلكتروني |
| 4 | |

### 5.3 الاعتماد

| الاسم | الوظيفة | رقم القرار | التاريخ |
|---|---|---|---|
| د. نهاد بنت عبد الله العمير | نائب الرئيس للتطوير والشراكة المجتمعية | 61945 | 2024/03/06 |

## 4. المقدمة

تعتبر حماية المعلومات والأصول المعلوماتية والتقنية أمر ضروري لنجاح الجامعة؛ ولهذه الغاية تقوم إدارة الأمن السيبراني بتطوير وإنشاء وتنظيم العمليات الأمنية المطلوبة لحماية الأصول المعلوماتية والتقنية، وتحدد هذه الوثيقة سياسة العمل عن بعد داخل الجامعة وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

تُدرج هذه السياسة في إطار سياسة الجامعة وتحت الصلاحيات الممنوحة من صاحب الصلاحية من تاريخ اعتمادها.

## 5. الهدف

الغرض من سياسة العمل عن بعد هو توفير التوجيه والمتطلبات الأمنية لجميع المستخدمين بشأن مسؤولياتهم والتزاماتهم فيما يتعلق باستخدام أصول وبيانات الجامعة في العمل عن بعد.

## 6. قابلية التطبيق ونطاق العمل

تنطبق أحكام هذه السياسة على جميع العاملين أو المكلفين الذين يعملون في الجامعة سواء بعقود دائمة أو مؤقتة وبشكل مباشر أو غير مباشر بما في ذلك الموردين والمقاولين الخارجيين وأي شخص لديه صلاحية الوصول الدائم أو المؤقت إلى بيانات الجامعة مهما كان مصدرها أو شكلها أو طبيعتها وإلى أنظمة وأجهزة وقواعد بيانات الجامعة.

## 7. السياسة

### 1.7 متطلبات السياسة العامة

1.1.7 يجب الحصول على موافقة إدارة الأمن السيبراني في الجامعة لطلبات الوصول لأنظمة العمل عن بعد ويكون ذلك بعد تقديم المبررات اللازمة.

2.1.7 يجب أن تقوم إدارة الأمن السيبراني في الجامعة بمراجعة طلبات الوصول لأنظمة العمل عن بعد مع الاخذ في الاعتبار عند المراجعة تصنيف البيانات وحساسية الأصول التقنية والمعلوماتية.

3.1.7 يجب تحديد البيانات المصنفة التي يمكن استخدامها أو الوصول إليها أو التعامل معها من خلال أنظمة العمل عن بعد وحمايتها باستخدام الضوابط التقنية اللازمة مثل (Prevention Data Leakage) وغيرها من التقنيات من خلال تحليل المخاطر السيبرانية للجامعة.

4.1.7 في حالة السماح باستخدام الأجهزة الشخصية في العمل عن بعد فيجب أن يكون الجهاز المستخدم في العمل عن بعد مستوفياً للمتطلبات الأمنية التي وضعها الجامعة.

5.1.7 يجب إدارة الأجهزة المحمولة وأجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة Mobile device Management (MDM) .

6.1.7 يجب تطبيق جميع الضوابط الأمنية اللازمة بما يتماشى مع متطلبات الأجهزة المحمولة المنصوص عليها في سياسة أمن الأجهزة المحمولة والأجهزة الشخصية.

7.1.7 يجب على الموظف التأكد من توفير الحماية اللازمة للأجهزة المحمولة في الأماكن العامة.

8.1.7 تحديث الحزم الأمنية للأصول التقنية والأنظمة المستخدمة للدخول عن بعد وتحديثها بشكل دوري على ألا تقل عن مرة واحدة، كل سنة.

9.1.7 يجب مراجعة وتحصين الإعدادات المصنعية (Default Configuration) التقنية لأنظمة العمل عن بعد، ومنها وجود كلمات مرور ثابتة، وخلفية افتراضية.

10.1.7 يجب ضمان تطبيق متطلبات الإدارة الآمنة للجلسات (Management Session Secure) وتشمل:

- موثوقية الجلسة (Authenticity)
- اقفال الجلسة (Lockout)
- انهاء مهلة الجلسة (Timeout)

11.1.7 يجب تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.

12.1.7 يجب تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد، وخصوصاً على الأنظمة الداخلية، وفتحها حسب الحاجة.

13.1.7 يجب مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) ذات العلاقة بأنظمة العمل عن بعد بشكل دوري.

14.1.7 يجب توفير الحماية من هجمات تعطيل الخدمات الموزعة (Distributed of denial of services) على أنظمة العمل عن بعد للحد من المخاطر السيبرانية الناتجة عن هجمات تعطيل الخدمات.

15.1.7 يجب توفير الحماية من التهديدات المتقدمة المستمرة على مستوى شبكة أنظمة العمل عن بعد ( Network APT).

## 2.7 حماية البيانات والمعلومات

1.2.7 يجب أن تكون أقراص الأجهزة المستخدمة في العمل عن بعد مشفرة بشكل كامل.

2.2.7 يجب عمل النسخ الاحتياطي على فترات زمنية مخطط لها لأنظمة العمل عن بعد بناء على تقييم أخطار الأمن السيبراني للجامعة.

3.2.7 يجب إجراء فحص دوري؛ لتحديد مدى فعالية استعادة النسخ الاحتياطية الخاصة بأنظمة العمل عن بعد.

4.2.7 يجب استخدام طرق وخوارزميات محدثة وآمنة للتشفير على كامل الاتصال الشبكي المستخدم للعمل عن بعد.

5.2.7 يجب أن يتم حذف المعلومات الخاصة بالجامعة المخزنة على الأجهزة المستخدمة في العمل عن بعد في الحالات التالية:

- فقدان الجهاز او سرقته
- الاشتباه بوجود خطر أمني على الجهاز
- انتهاء علاقة الموظف بالجامعة

6.2.7 الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم المستخدمة في عمليات الدخول عن بعد باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.

## 3.7 إدارة أخطار الأمن السيبراني

1.3.7 يجب تقييم أخطار الأمن السيبراني لأنظمة العمل عن بعد بشكل دوري.

2.3.7 يجب تقييم أخطار الأمن السيبراني عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام.

3.3.7 يجب تضمين أخطار الأمن السيبراني الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد في سجل أخطار الأمن السيبراني الخاص بالجامعة.

## 4.7 إدارة الأصول

1.4.7 يجب تحديد وحصر الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد، وتحديثها بشكل دوري.

## 5.7 إدارة التحكم في الوصول

1.5.7 يجب إدارة صلاحيات المستخدمين للعمل عن بعد بناءً على احتياجات العمل، مع مراعاة حساسية الأنظمة ومستوى الصلاحيات، ونوعية الأجهزة المستخدمة من قبل العاملين للعمل عن بعد.

2.5.7 يجب تقييد إمكانية الوصول عن بعد لنفس المستخدم من أجهزة حاسبات متعددة في نفس الوقت (Concurrent Logins).

3.5.7 يجب استخدام معايير آمنة لإدارة الهويات وكلمات المرور المستخدمة في أنظمة العمل عن بعد.

4.5.7 تطبيق التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد.

5.5.7 يجب مراجعة هويات الدخول والصلاحيات المستخدمة للعمل عن بعد بشكل دوري.

### 6.7 إدارة الثغرات واختبار الاختراق

1.6.7 يجب فحص الثغرات واكتشافها على أنظمة العمل عن بعد وتصنيفها حسب خطورتها مرة واحدة كل ثلاثة أشهر على الأقل.

2.6.7 تكون معالجة الثغرات على أنظمة العمل عن بعد، مرة واحدة كل ثلاثة أشهر على الأقل.

3.6.7 يجب أجراء اختبار للاختراق مرة واحدة سنويا على الأقل لأنظمة العمل عن بعد على أن تشمل اختبارات الاختراق جميع المكونات التقنية لأنظمة العمل عن بعد.

### 7.7 الحوسبة السحابية والاستضافة

1.7.7 يجب أن تكون موقع استضافة أنظمة العمل عن بعد داخل المملكة العربية السعودية.

### 8.7 التوعية والتدريب

1.8.7 يجب أن يتم تقديم التوجيه اللازم للعاملين في الجامعة على المهارات التقنية اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند التعامل مع أنظمة العمل عن بعد.

### 9.7 مراقبة الأمن السيبراني وحوادث وتهديدات الأمن السيبراني

1.9.7 يجب تفعيل سجلات الأحداث الخاصة بالأمن السيبراني على الأصول التقنية وأنظمة العمل عن بعد ومراقبتها على مدار الساعة.

2.9.7 يجب تحليل ومراقبة سلوك مستخدمي أنظمة العمل عن بعد (User Behavior Analytics UBA).

3.9.7 يجب تحديث إجراءات مراقبة الأمن السيبراني على مدار الساعة وتطبيقها، بحيث تشمل مراقبة عمليات الدخول عن بعد، ولا سيما عمليات الدخول عن بعد من خارج المملكة والتحقق من صحتها.

4.9.7 يجب الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني لأنظمة العمل عن بعد لمدة لا تقل عن 12 شهر حسب المتطلبات التشريعية والتنظيمية ذات العلاقة.

5.9.7 يجب تحديث خطط الاستجابة لحوادث الأمن السيبراني ومعلومات التواصل داخل الجهة بما يتوافق مع حالة العمل عن بعد، بما يضمن القدرة على التواصل وجاهزية فرق الاستجابة للحوادث.

6.9.7 يجب الحصول على المعلومات الاستباقية (Threat Intelligence) ذات العلاقة بأنظمة العمل عن بعد بشكل دوري والتعامل معها.

7.9.7 يجب تنفيذ وتطبيق التوصيات والتنبيهات الخاصة بحوادث وتهديدات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني.

## 8. الأدوار والمسؤوليات

**يجب على إدارة الأمن السيبراني:**

1.1.8 على مدير الأمن السيبراني اعتماد السياسة من صاحب الصلاحية والعمل على تنفيذها.

2.1.8 على مدير الأمن السيبراني اعتماد المعايير والإجراءات والتوجيهات لضمان الالتزام الضروري بمتطلبات أمن عمليات الجامعة.

3.1.8 على مدير الأمن السيبراني ضمان التوافق بين هذه السياسة وأعمال الجامعة.

4.1.8 على مدير الأمن السيبراني حل أي متعارضات تنشأ عن هذه السياسة.

5.1.8 على مدير الأمن السيبراني توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة حيثما أمكن.

6.1.8 على إدارة الأمن السيبراني تعميم سياسة الالتزام بالأمن السيبراني وحوكمة البيانات على جميع إدارات وموظفي ومستخدمي الجامعة المصرح لهم أو الذين سيصرح لهم الوصول إلى الأصول التقنية والمعلوماتية.

7.1.8 على إدارة الأمن السيبراني التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

8.1.8 على إدارة الأمن السيبراني مراجعة السياسة بشكل دوري وفقًا للخطة الزمنية التي تم تحديدها.

**يجب على عمادة الاتصالات وتقنية المعلومات:**

9.1.8 الالتزام بهذه السياسة، وتنفيذ الضوابط المذكورة في هذه السياسة وكذلك الإبلاغ عن أي حادث أمني لإدارة الأمن السيبراني.

**يجب على الإدارة العليا ومدراء الإدارات ورؤساء الوحدات والمستشارين ما يلي:**

10.1.8 التأكد من مشاركة هذه السياسة لجميع العاملين داخل الجامعة أو الملف.

11.1.8 إبلاغ إدارة الأمن السيبراني عن أي تجاوزات أو عدم التزام بهذه السياسة.

**يجب على العاملين في الجامعة الالتزام بأحكام هذه السياسة والإبلاغ عن أي حادث أمني أو عدم التزام بأي أحكام واردة في هذه السياسة الى مدير الأمن السيبراني.**

## 9. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

## 10. تغييرات السياسة

يجب مراجعة السياسة سنويًا على الأقل أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية، وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية في الجامعة.

## 11. الالتزام

يجب على جميع العاملين في الجامعة والأطراف (الخارجية/المتعاقد معهم) الالتزام بأحكام هذه السياسة، ويجب على مدير الأمن السيبراني في الجامعة ضمان المراقبة المستمرة للالتزام، ورفع التقارير اللازمة بهذا الشأن لصاحب الصلاحية بشكل دوري.

يجب اتخاذ الإجراءات اللازمة لضمان الالتزام بأحكام هذه السياسة، وذلك من خلال قيام إدارة الأمن السيبراني أو الإدارات ذات العلاقة بمراجعة دورية، واتخاذ إجراءات تصحيحية من قبل صاحب الصلاحية في الجامعة وفقاً للتوصيات المقدمة من قبل مدير الأمن السيبراني حيال أي انتهاك لأي من أحكام هذه السياسة، على أن تكون الإجراءات التأديبية متناسبة مع خطورة الحادثة وفقًا لما يسفر عنه التحقيق بهذا الخصوص، وتتضمن الإجراءات التأديبية على سبيل المثال لا الحصر الآتي:

- سحب صلاحية الوصول إلى البيانات وأصول تقنية المعلومات وأنظمة الجامعة المتصلة بها.
- توجيه إنذار خطي، أو إنهاء خدمة العامل أو حسب ما يراه الجامعة من إجراءات مناسبة.

يستوجب عدم الالتزام بأي من أحكام هذه السياسة -دون الحصول على استثناء مسبق من إدارة الأمن السيبراني اتخاذ الإجراءات المناسبة وفقًا للسياسات واللوائح المعمول بها في الجامعة، أو حسبما يكون مناسبًا، ووفقًا للشروط التعاقدية مع أي أشخاص أو جهات متعاقد معهم.

## 12. السياسات والمعايير والإجراءات ذات العلاقة

- DICT.I.06-01.CS.A. V2.0- السياسة العامة للأمن السيبراني وحوكمة البيانات
- DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني وحوكمة البيانات
- DICT.I.06-24.CS.A. V2.0- سياسة إدارة مخاطر الأمن السيبراني
- DICT.I.06-32.CS.A. V2.0- سياسة الأمن المادي والبيئي
- DICT.I.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- DICT.I.06-29.CS.A. V2.0- سياسة التشفير
- DICT.I.06-09.CS.A. V2.0- سياسة إدارة حوادث الأمن السيبراني
- DICT.I.06-10.CS.A. V2.0- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-05.CS.A. V2.0- سياسة إدارة الثغرات واختبار الاختراق
- DICT.I.06-30.CS.A. V2.0- سياسة الحماية من البرمجيات الضارة
- DICT.I.06-42.CS.A. V2.0- سياسة أمن الأجهزة المحمولة والأجهزة الشخصية
- DICT.I.06-04.CS.A. V2.0- سياسة إدارة الأصول
- DICT.I.06-33.CS.A. V2.0- سياسة التحكم في الوصول
- DICT.I.06-49.CS.A.V2.0- معايير إدارة هويات الدخول والصلاحيات
- DICT.I.06-50.CS.A.V2.0- معايير الأمن المادي
- DICT.I.06-60.CS.A.V2.0- معايير تصنيف الأصول
- DICT.I.06-63.CS.A.V2.0- معايير إدارة الثغرات واختبار الاختراق
- DICT.I.06-67.CS.A.V2.0- معايير إدارة حوادث الأمن السيبراني
- DICT.I.06-71.CS.A.V2.0- معايير التشفير
- DICT.I.06-68.CS.A.V2.0- معايير إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-62.CS.A.V2.0- معايير إدارة الأصول
- DICT.I.06-72.CS.A.V2.0- معايير الحماية من البرمجيات الضارة
- DICT.I.06-79.CS.A.V2.0- معايير أمن الأجهزة المحمولة والأجهزة الشخصية
- DICT.I.04-40.CS.A.V2.0- إجراءات إدارة مخاطر الأمن السيبراني
- DICT.I.04-37.CS.A.V2.0- إجراءات الحماية من البرمجيات الضارة

## 13. المراجع

| اسم القسم | الضوابط الأساسية للأمن السيبراني | ضوابط الأمن السيبراني للأنظمة الحساسة | ضوابط الأمن السيبراني للعمل عن بعد | ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات | ضوابط الأمن السيبراني للحوسبة السحابية | الآيزو 27001:2013 | المعهد الوطني للمعايير والتقنية |
|---|---|---|---|---|---|---|---|
| العمل عن بعد | 1-3-1 | 1-3-1 | 2-1<br>3-1<br>1-2<br>2-2<br>3-2<br>4-2<br>5-2<br>6-2<br>7-2<br>8-2<br>9-2<br>10-2<br>11-2<br>12-2<br>1-3 | - | - | A.6.2.2 | - |

----------نهاية الوثيقة----------