



سياسة الاستخدام المقبول للأصول



قائمة المحتويات

2	الأهداف
2	نطاق العمل وقابلية التطبيق
3	الأدوار والمسؤوليات
6	بنود السياسة
9	بيانات السياسة
10	2.4 تداول المعلومات
12	5.4 سياسة تنظيف مكان العمل
12	6.4 إعدادات أنظمة المعلومات
13	7.4 استخدام الوسائط المحمولة
14	8.4 استخدام الحواسيب المكتبية
15	9.4 إدارة كلمات المرور
16	10.4 سياسة استخدام الانترنت
17	11.4 استخدام البريد الإلكتروني
18	12.4 عناصر التحكم الأمنية المتعلقة بالاجتماعات والمؤتمرات
18	13.4 الأمن المادي
19	14.4 الانتهاكات الأمنية
20	15.4 استخدام وسائل التواصل الاجتماعي
22	تنفيذ السياسة والالتزام بها
22	معييار الاستثناءات المتعلقة بهذه السياسة
22	مراجع ISO27001
22	مراجع إطار الهيئة الوطنية للأمن السيبراني
22	السياسات ذات الصلة
22	مراجعة الوثيقة
23	التعريفات

الأهداف

تهدف هذه السياسة إلى إدارة قواعد الاستخدام المقبول للأصول المعلوماتية ومرافق معالجة البيانات في جامعة حفر الباطن. و يُعتبر استخدام أي أصل من الأصول المعلوماتية في جامعة حفر الباطن بمثابة الموافقة على هذه السياسة. كما تساهم هذه السياسة في فهم المستخدمين للمتطلبات الأمنية والسياسات التي يجب اتباعها خلال أنشطة العمل اليومية وتقدم التدابير الوقائية / والتصحيحية لتقليل المخاطر المتعلقة بإساءة استخدام أصول المعلومات ومرافق معالجة المعلومات

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٣-١-٢ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

أهداف هذه السياسة هي:

- وضع معايير استخدام مقبولة لموارد المعلومات والمعلومات في جامعة حفر الباطن.
- تعزيز والحفاظ على بيئة تثق فيها الإدارة والمستخدمون في أمن هذه الموارد.
- ضمان استيفاء متطلبات تأمين الأجهزة المادية و تراخيص البرامج.
- تحقيق الاتساق في الضوابط المتعلقة بأصول المعلومات ومرافق معالجة المعلومات.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع موظفي جامعة حفر الباطن المعيّنين من قبل جامعة حفر الباطن بشكل مباشر أو غير مباشر، بالإضافة إلى كافة الجهات الخارجية الذين يمتلكون أو يستخدمون معلومات و/ أو مرافق مملوكة لجامعة حفر الباطن .

يشمل مصطلح "مرافق المعلومات"، على سبيل المثال لا الحصر:

- أجهزة الكمبيوتر الشخصية / أجهزة الكمبيوتر المحمولة (المتصلة بالشبكة والمستقلة)
- البنية التحتية للشبكة (بما في ذلك معدات الشبكات ومنافذ البيانات وكابلات التوصيل وما إلى ذلك)
- الأدوات والبرامج الداخلية.
- خوادم التطبيقات.
- خوادم قواعد البيانات.
- خوادم الإنترنت.
- بوابات الوصول إلى الشبكات الخارجية و الإنترنت.
- خوادم البريد الإلكتروني.

ملحوظة: تنطبق هذه السياسة على أنظمة الجامعة وكذلك المنصات السحابية.

الأدوار والمسؤوليات

يجب أن يكون لكل وظيفة متضمن في هذه السياسة مسؤوليات رئيسية على النحو التالي:

الدور	المسؤولية
اللجنة الإشرافية للأمن السيبراني	- القيادة و الإشراف على تنفيذ سياسة الاستخدام المقبول. - الإشراف على تأمين و حماية معلومات و تقنيات جامعة حفر الباطن نيابةً عن جامعة حفر الباطن و إدارته. - يجب أن تكون هذه اللجنة هيئة لها سلطة في إتخاذ القرار بما يتعلق في أي تغييرات رئيسية في سياسة الاستخدام المقبول. - تحرص اللجنة على التأكد من توافق سياسة الاستخدام المقبول مع إطار التزام الهيئة الوطنية للأمن السيبراني و كذلك المتطلبات القانونية و التنظيمية و التعاقدية. - هذه اللجنة مسؤولة عن مراجعة واعتماد هذه السياسة والاستثناءات المتعلقة بها.
حوكمة و التزام الأمن السيبراني	- تطوير و مراجعة و تحديث و نشر سياسات الاستخدام المقبول و ضمان التوافق مع المعايير الرائدة و الإلتزام للقوانين و اللوائح التنظيمية. - قيادة تطبيق سياسات الاستخدام المقبول والإجراءات المتعلقة بها داخل بيئة جامعة حفر الباطن. - التنسيق مع الإدارات المختلفة مثل إدارة تقنية المعلومات و الأمن المادي وغيرها من الإدارات و ذلك للتأكد من توافق سياسة الاستخدام المقبول مع السياسات الأخرى و الإجراءات و الضوابط المطبقة داخل جامعة حفر الباطن. - تنفيذ و متابعة كافة مراجعات الإلتزام المتعلقة بضوابط سياسة الاستخدام المقبول. - التنسيق مع أصحاب المصلحة المعنيين لضمان معالجة الثغرات ضمن الجدول الزمني المحدد. - قيادة برنامج التوعية الأمنية والتعليم والتدريب المتعلق بسياسة الأمن السيبراني بمشاركة رأس المال البشري. - التأكد من تطبيق الضوابط التي تغطيها سياسة الاستخدام المقبول بصورة فعالة.

• تطوير الإجراءات بالتوافق مع سياسة الاستخدام المقبول.	
• التأكد من قيام جميع موظفي جامعة حفر الباطن أو الأطراف الخارجية بالتوقيع على اتفاقيات السرية وعدم الإفصاح التي تتضمن بالتفصيل الاستخدام المقبول لأصول و مرافق معالجة المعلومات أثناء العمل مع جامعة حفر الباطن. • التنسيق مع إدارة الحوكمة و الالتزام وتنظيم جلسات و تدريبات توعية بالأمن السيبراني و التي تتضمن سياسة الاستخدام المقبول لأصول و مرافق معالجة المعلومات. • التنسيق مع إدارة الأمن السيبراني، الشؤون القانونية والإدارة العليا في حالة الحاجة لإجراءات تأديبية ضد موظف أو طرف خارجي في حالات انتهاك سياسة الاستخدام المقبول. • تطوير الإجراءات وفقاً لهذه السياسة.	رأس المال البشري
• التأكد من توقيع الجهات الخارجية على اتفاقية عدم الإفشاء قبل منحهم صلاحية الوصول إلى معلومات جامعة حفر الباطن. • إعداد الإرشادات الخاصة بالاستخدام الشخصي لموارد جامعة حفر الباطن . • تحديد تصنيف أصول المعلومات ووسمها لضمان تنفيذ الضوابط الأمنية المناسبة بناءً على تصنيف أصول جامعة حفر الباطن المحدد في سياسة إدارة الأصول. • في حالة وجود أي مخالفة، يجب التنسيق مع الجهة المختصة لتنفيذ أي إجراء تأديبي مطلوب. • تطوير الإجراءات وفقاً لهذه السياسة.	مدراء الإدارات / مدراء المشروع / ملاك الأصول
• مسؤول عن تنفيذ جميع الضوابط المادية والبيئية وذلك لحماية أصول المعلومات و مرافق جامعة حفر الباطن. • ضمان الاستخدام المقبول لأصول المعلومات ومرافق المعالجة من خلال مراقبة المستخدمين الداخلون إلى مقر جامعة حفر الباطن والخارجون منها. • التنسيق مع فريق الحوكمة و الالتزام لتنفيذ ضوابط بيئة العمل النظيفة بما في ذلك سطح المكتب النظيف. • تطوير الإجراءات وفقاً لهذه السياسة.	الأمن المادي
تقديم الدعم في تحديد احتياجات ومتطلبات معمارية الأمن السيبراني.	معمارية الأمن السيبراني

• تنفيذ متطلبات الأمن السيبراني طبقاً لمعمارية الأمن السيبراني المرجعية. • التنسيق مع فريق إدارة المخاطر لتحديد مجالات المخاطر ومعالجتها بتنفيذ متطلبات الأمن السيبراني المستحدثة كلما أمكن. • تطوير الإجراءات بالتوافق مع هذه السياسة.	
• يجب إخطار موظفي إدارة الدعم الفني باستثناءات هذه السياسة والحصول على الموافقة لذلك. • الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه فيها الدعم الفني للمستخدمين. • استخدام المعلومات للأغراض المخصصة فقط من قبل جامعة حفر الباطن. • تحمل مسؤولية كافة الأنشطة المتعلقة باستخدام مميزات الوصول.	موظفو جامعة حفر الباطن / الجهات الخارجية



بنود السياسة

البند العامة

- 1-1 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بجامعة حفر الباطن بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.
- 2-1 يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.
- 3-1 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
- 4-1 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.
- 5-1 يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مسؤوليه.
- 6-1 يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.
- 7-1 يمنع الإفصاح عن أي معلومات تخص جامعة حفر الباطن، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواء كان ذلك داخلياً أو خارجياً.
- 8-1 يُمنع نشر معلومات تخص جامعة حفر الباطن عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.
- 9-1 يُمنع استخدام أنظمة جامعة حفر الباطن وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة حفر الباطن.
- 10-1 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة حفر الباطن دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).
- 11-1 يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بجامعة حفر الباطن، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة حفر الباطن.
- 12-1 تحتفظ <الإدارة المعنية بالأمن السيبراني> بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييرها.
- 13-1 يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.
- 14-1 يجب ارتداء البطاقة التعريفية في جميع مرافق جامعة حفر الباطن.
- 15-1 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> في حال فقدان المعلومات أو سرقتها أو تسريبها.

2- حماية أجهزة الحاسب الآلي

- 1-2 يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

2-2 يمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من <الإدارة المعنية بالأمن السيبراني>، بما في ذلك الأنشطة التي تُمكن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

3-2 يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

4-2 يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

5-2 يمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من <الإدارة المعنية بتقنية المعلومات>.

6-2 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بـ جامعة حفر الباطن أو أصولها.

3- الاستخدام المقبول للإنترنت والبرمجيات

1-3 يجب إبلاغ <الإدارة المعنية بالأمن السيبراني> في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

2-3 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

3-3 يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

4-3 يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

5-3 يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

6-3 يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة حفر الباطن دون الحصول على تصريح مسبق من <الإدارة المعنية بتقنية المعلومات>.

7-3 يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

8-3 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

9-3 يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة حفر الباطن وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

10-3 يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

11-3 يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

4- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

1-4 يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييرها.

2-4 يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

3-4 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

4-4 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بجامعة حفر الباطن في أي موقع ليس له علاقة بالعمل.

5-4 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة حفر الباطن أو أصولها.

6-4 تحتفظ جامعة حفر الباطن بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية و<الإدارة المعنية بالأمن السيبراني> وفقاً للإجراءات والتنظيمات ذات العلاقة.

7-4 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

5- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

1-5 يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

2-5 يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

6- استخدام كلمات المرور

1-6 يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة حفر الباطن وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

1-6 يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو <الإدارة المعنية بتقنية المعلومات>.

2-6 يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

بيانات السياسة

السياسة الفعالة هي نتاج مجهود فريق يدعمه ويسانده كل موظف يتعامل مع المعلومات و/ أو أنظمة المعلومات في جامعة حفر الباطن. لذا يجب على كل مستخدم حاسوب معرفة هذه التوجيهات وتأدية الأنشطة الخاصة به وفقاً لها.

1-4 المسؤوليات العامة

- 4.1.1 استخدام نظم المعلومات ومرافق معالجة المعلومات الخاصة لجامعة حفر الباطن ومسؤوليات المستخدم.
- 2.1.4 يجب على المستخدم تقييم مدى إمكانية الاستخدام الشخصي (الذي لا يؤثر على موارد جامعة حفر الباطن). ويجب على الإدارات إعداد الإرشادات المتعلقة بالاستخدام الشخصي للأنظمة الداخلية/ الخارجية/ أنظمة الشبكة الداخلية. في حالة غياب هذه السياسات يجب على الموظفين استشارة مشرفيهم أو مديريهم الذين بالتبعية و كذلك استشارة مسئولين إدارة الحوكمة و الالتزام للمساعدة.
- 3.1.4 يتحمل المستخدمون النهائيون مسؤولية فهم واتباع سياسات أمن المعلومات الخاصة بجامعة حفر الباطن من حيث صلتها بحماية أصول المعلومات.
- 4.1.4 يحظر على المستخدمين إرسال أي بيانات رسمية حساسة إلى البريد الإلكتروني الشخصي أو أي مرفق تخزين سحابي عام.
- 5.1.4 يتعين على المستخدمين فهم التعريف وتصنيف البيانات المحدد في سياسة إدارة الأصول والتصرف وفقاً لذلك.
- 6.1.4 استخدام الأجهزة المحمولة محظور تمامًا في جامعة حفر الباطن إلا باستثناء معتمد من قبل مالك الأصول والإدارة العليا.
- 7.1.4 محتوى أي معلومات متاحة للموظفين الآخرين أو الأطراف الخارجية عبر شبكة جامعة حفر الباطن هي مسؤولية مدير المشروع الذي يتعامل مع المشروع أو المستخدم الذي يرسل المعلومات.
- 8.1.4 لا يجوز للمستخدمين استخدام موارد جامعة حفر الباطن (بما في ذلك الماسحات الضوئية، وأجهزة الفاكس ، والطابعات ، وما إلى ذلك) في أعمالهم الشخصية ، كما أنهم مسؤولون عن اتباع السياسة الخاصة باستخدام هذه المرافق.
- 9.1.4 يجب على المستخدمين النهائيين عدم إتلاف أو تغيير أو تعطيل أي من الأصول المادية لجامعة حفر الباطن .
- 10.1.4 يحظر على المستخدمين إحضار أو استخدام أي أجهزة حوسبة شخصية / وسائط تخزين مثل الأقراص المضغوطة / أقراص الفيديو الرقمية ومحركات أقراص USB ومحركات الأقراص الثابتة وأجهزة الكمبيوتر المحمولة وما إلى ذلك داخل مباني جامعة حفر الباطن ما لم تصرح بذلك الإدارة وفقاً لعملية الاستثناء.
- 11.1.4 يتعين على المستخدمين تمزيق أي مستند حساس لم يعد مطلوبًا. يجب أن توضع النسخ المطبوعة من البيانات الرسمية (إذا كانت لن تستخدم مستقبلاً) في صندوق - تمزيق الأوراق. كما يجب على المستخدمين عدم ترك

- المستندات المطبوعة التي تحتوي على معلومات حساسة على الطابعة ، ويجب أخذ أي منهما على الفور من الطابعة و يجب أن يكون في صندوق تمزيق الأوراق إذا لم يتم استخدامه.
- 12.1.4 يجب أن يدرك المستخدمون أن فريق الحوكمة والالتزام أو فريق المراجعة الداخلية قد يقوم بمراجعة أنشطة المستخدمين ومراقبتها وتسجيلها، مع أو بدون إشعار ، إذا كان الموقف يستدعي تحقيقاً فورياً أو إضافياً.
- 13.1.4 يجب على جميع المستخدمين الإبلاغ عن أي نقاط ضعف / حوادث أمنية ملحوظة (أو مشتبه بها) إلى قسم الدعم الفني للمستخدمين في أسرع وقت ممكن.
- 14.1.4 يتحمل المستخدم المسؤولية عن التسبب في أي اضطراب في العمليات أو التسبب في أي ضرر لسمعة جامعة حفر الباطن أثناء استخدام موارد جامعة حفر الباطن للاستخدام الشخصي المسموح به.
- 15.1.4 يجب أن يوقع جميع المستخدمين الذين يتمتعون بصلاحيات الوصول إلى أنظمة المعلومات ومرافق معالجة البيانات في جامعة حفر الباطن ، التوقيع على اتفاقية عدم الإفشاء كجزء من عقد توظيفهم. يتعين على الأطراف الخارجية التوقيع على مثل هذه الاتفاقيات قبل منحهم صلاحية الوصول إلى أنظمة معلومات جامعة حفر الباطن.
- 16.1.4 يُحظر تمامًا مشاركة المعلومات الحساسة الخاصة بجامعة حفر الباطن أو توزيعها ما لم يتم التصريح بذلك من قبل السلطة المخولة.
- 17.1.4 يجب أن يوافق مدير / مالك المشروع المعني على أي استخدام لموارد معلومات جامعة حفر الباطن من قبل أطراف خارجية، ويجب مراجعة صلاحيات و أنشطة الوصول بدقة.

2.4 تداول المعلومات

- 1.2.4 الالتزام بمستويات سرية المعلومات
- 2.2.4 يجب أن يفهم جميع مستخدمي الأصول مستويات سرية المعلومات في جامعة حفر الباطن وأن يلتزموا بتلك المستويات.
- 3.2.4 في حالة الشك، يتعين على المستخدمين سؤال مدراءهم عما إذا كانوا يمتلكون صلاحية الوصول للمعلومات أم لا.
- 4.2.3 يجب أن يتأكد المستخدمون من توزيع جميع أصول معلومات جامعة حفر الباطن على أساس الاحتياج لمعرفة تلك المعلومات، مع الأخذ في الاعتبار اتخاذ تدابير الحماية اللازمة.
- 5.2.4 يجب أن يتأكد المستخدمين من التخلص الآمن لجميع أصول المعلومات وفقاً لدرجة تصنيفها ومدة البقاء الخاصة بها.
- 6.2.4 يجب أن تتضمن جميع تطبيقات الويب الخارجية إعلاناً يوضح سياسة الاستخدام الآمن للمستخدمين والتي يجب أن يلتزم بها المستخدم الذي يصل إلى التطبيق.

7.2.4 يحظر على المستخدمين استخدام أي آليات غير مصرح بها لمشاركة الملفات مثل البرامج التالية (peer-to-peer)، web messenger، file shares، وبرامج المجانية لمشاركة الملفات عبر الانترنت وغيرها). كما يحظر على المستخدمين مشاركة الملفات باستخدام أجهزة متنقلة مثل وحدات التخزين (USB's)، والأقراص الصلبة الخارجية (external drives)، والأقراص المدمجة (CDs)، وأقراص الفيديو الرقمية (DVDs) دون الحصول على الموافقات اللازمة.

8.2.4 يجب على جميع الموظفين و الأطراف الخارجية الالتزام بقواعد وضع تصنيف درجة السرية لجميع أصول المعلومات.

9.2.4 يجب على جميع مستخدمي جامعة حفر الباطن الذين يستخدمون الأصول إبلاغ المدير أو رئيس القسم أو إدارة الحوكمة و الالتزام عن غياب تصنيف درجة السرية إذا تمت ملاحظة ذلك لأي من الأصول.

3.4 التوعية بشأن الهندسة الاجتماعية

1.3.4 يجب أن يحضر جميع المستخدمين جلسات التوعية الأمنية السنوية ويجتازوا الاختبار بواسطة فريق الأمن السيبراني.

2.3.4 يجب أن يكون جميع مستخدمي الأصول على دراية بتقنيات الهندسة الاجتماعية، حيث يستخدم المحتالين التواصل الاجتماعي والموارد الخارجية لجمع معلومات سرية من الموظفين أو الأطراف الخارجية في جامعة حفر الباطن.

3.3.4 يجب أن يبذل المستخدم العناية اللازمة أثناء استخدام البريد الإلكتروني، حيث إن الهندسة الاجتماعية يمكن أن تحدث أيضًا عبر البريد الإلكتروني من أجل جمع المعلومات السرية. فقد اعتاد المستخدمين على البريد الإلكتروني لدرجة أنهم لا يتأكدون من سلامة مصدر أو محتوى رسائل البريد الإلكتروني، لذا يجب تغيير ذلك.

4.4 تبادل المعلومات

- 1.4.4 يحظر على المستخدمين مناقشة المعلومات الحساسة في الحالات التالية:
- في حالة وجود أي شخص غريب أو موظف ليست لديه صلاحية معرفة تلك المعلومات.
 - في الأماكن العامة مثل منطقة التدخين والكافتيريا والمطاعم والنوادي وغيرهم.
 - أثناء استخدام قنوات الاتصالات العامة مثل الجوالات والرسائل القصيرة وغيرها.
 - عند استخدام عنوان الاتصالات التي تعتمد على الانترنت مثل المنتديات العامة ومواقع المدونات ومواقع الشبكات الاجتماعية والقائمة البريدية العامة وغير ذلك.

5.4 سياسة تنظيف مكان العمل

1.5.4 يجب على جميع المستخدمين تنفيذ سياسة تنظيف مكان العمل (امتداد لسياسة المكتب النظيف) عند مغادرة مكان عملهم الذي يمكن الوصول إليه أو دخوله من قبل أشخاص آخرين، لمنع الوصول غير المصرح به لأصول المعلومات.

2.5.4 تتضمن أصول المعلومات التي تتطلب حماية ما يلي (على سبيل المثال لا الحصر):

- الوثائق التي تحتوي على معلومات محظورة أو سرية.
- الحواسيب المحمولة.
- وسائط التخزين والأجهزة التي تحتوي على معلومات محظورة أو سرية.
- معدات الفحص والتحكم.
- الأجهزة الإلكترونية المحمولة المقدمة من قبل جامعة حفر الباطن.

3.5.4 يجب أن تتضمن الإجراءات الوقائية المتعلقة بالالتزام بسياسة المكتب النظيف والشاشة النظيفة على ما يلي وعلى الأقل (على سبيل المثال لا الحصر):

- يجب حفظ النسخ الورقية في خزانة أو دولاب والإغلاق عليها.
- يجب حفظ الأصول المنقولة القيمة في خزانة أو دولاب والإغلاق عليها.
- يجب إغلاق أبواب المكاتب لمنع أي دخول غير مصرح به.
- يجب أن يتأكد المستخدمون من حماية رسائل الفاكس الصادرة والواردة وعدم تركها .
- يجب تعطيل الأجهزة القادرة على الطباعة والنسخ التلقائي.
- يجب إزالة المعلومات السرية والأصول المذكورة أعلاه من الأدراج فوراً.
- يجب تسجيل الخروج من الأنظمة والتطبيقات في حالة عدم استخدامها.
- يجب إغلاق الأنظمة وتفعيل شاشة التوقف لحماية أي معلومات خاصة أو سرية من الوصول غير المصرح به وفي حالة عدم وجود وسيلة للإغلاق يتم إنهاء الجلسة النشطة بعد فترة معينة من عدم النشاط.
- يجب أن يتأكد المستخدمون من وضع حواسيبهم بعيداً عن رؤية الأشخاص الغير المصرح لهم بالاطلاع على تلك المعلومات.
- يجب إزالة المعلومات الحساسة من الطابعات فور طباعتها.

6.4 إعدادات أنظمة المعلومات

1.6.4 يحظر على المستخدمين استخدام أي نظام حاسوب دون الحصول على تصريح من الجهات المعنية. ويعتبر الوصول غير المصرح به إلى أي ملف محمي أو مجزأ بمثابة انتهاك أمني خطير، قد يؤدي إلى اتخاذ إجراءات تأديبية.

2.6.4 يجب على المستخدمين التأكد من أنهم يستخدمون الحواسيب المكتبية والحواسيب المحمولة والأجهزة اللوحية الرسمية المقدمة من قبل جامعة حفر الباطن أثناء أنشطتهم اليومية.

3.6.4 يحظر على المستخدمين توصيل الحواسيب المكتبية أو الحواسيب المحمولة أو الأجهزة اللوحية الشخصية الخاصة بهم بشبكة جامعة حفر الباطن ، باستثناء هواتفهم المحمولة وتقتصر على شبكة W-LAN.

4.6.4 يحظر على المستخدمين تثبيت أو تحديث أو تغيير أي جهاز أو نظام تشغيل أو تطبيق أو برنامج على الحواسيب المكتبية أو الحواسيب المحمولة الخاصة بجامعة حفر الباطن باستثناء تلك المصرح بها من قبل إدارة الدعم الفني للمستخدمين.

5.4.6 يحظر على المستخدمين تجربة وتغيير إعدادات أي أجهزة أو أنظمة تشغيل أو تطبيقات أو برامج مثبتة على الحواسيب المكتبية أو الحواسيب المحمولة الرسمية الخاصة بجامعة حفر الباطن.

6.4.6 يحظر على المستخدمين تثبيت أو استخدام أي أنظمة تشغيل أو تطبيقات أو برامج غير مرخصة على الحواسيب المكتبية أو الحواسيب المحمولة الرسمية الخاصة بهم دون الحصول على تصريح بذلك. وفي حالة وجود أي استفسارات يتم التواصل مع نظام البلاغات الفنية في جامعة حفر الباطن.

7.4.6 يحظر على المستخدمين تخزين الملكيات الفكرية الخاصة بجامعة حفر الباطن مثل الشفرة البرمجية وغيرها، على الحواسيب المكتبية أو الحواسيب المحمولة الشخصية الخاصة بهم.

8.4.6 يجب على إدارة الدعم الفني للمستخدمين الاحتفاظ بنسخ احتياطية من ملفاتهم قبل تحديث الجهاز أو نظام التشغيل أو التطبيقات أو البرامج في الأنظمة التشغيلية الخاصة بهم من خلال استخدام محرك مشاركة الشبكة المخصص لذلك.

9.4.6 يجب على المستخدمين الاحتفاظ بمعلومات المشاريع على محرك مشاركة الشبكة المخصص لذلك وذلك لعمل نسخ احتياطية بشكل مستمر.

10.4.6 يحظر على المستخدمين تخزين أو معالجة أو نقل أي نسخ غير مصرح بها من تراخيص الوثائق والأجهزة والبرامج (انتهاك حقوق الملكية الفكرية وبراءات الاختراع) باستخدام موارد معلومات جامعة حفر الباطن.

11.4.6 يحظر على المستخدمين السماح لأي شخص غير مصرح له (بما في ذلك الزوج، أو الأقارب أو الأصدقاء) بالوصول إلى أي شبكة حاسوب حساسة.

7.4 استخدام الوسائط المحمولة

1.7.4 يجب على المستخدمين الاهتمام بشكل خاص بأي موارد حوسبة ، مثل أجهزة الكمبيوتر المحمولة ، والهواتف المحمولة ، وأجهزة الكمبيوتر المحمولة ، وما إلى ذلك لمنع تعريض معلومات العمل للخطر.

2.7.4 لا يجوز للمستخدمين الذين يحوزون أجهزة كمبيوتر محمولة أو هواتف محمولة وغيرها من أجهزة الكمبيوتر القابلة للنقل أو وسائط التخزين التي تحتوي على معلومات لجامعة حفر الباطن تركها دون مراقبة في أي وقت. إلا إذا تم قفل الجهاز لمنعه من السرقة، وتكون الشاشة مغلقة حسب المبادئ التوجيهية.

3.7.4 لا يجوز ترك المعلومات دون مراقبة في أي وقت. ما لم يكن من الممكن قفل الجهاز لمنعه من السرقة، ويتم إغلاق الشاشة وفقاً للإرشادات.

4.7.4 يجب على المستخدمين توخي عناية خاصة أثناء استخدام موارد الحوسبة المتنقلة في الأماكن العامة لحماية المعلومات من الوصول غير المصرح به.

5.7.4 لا يجوز للمستخدمين استخدام هواتفهم المحمولة الشخصية لتخزين أي معلومات رسمية

- 6.7.4. لا يجوز للمستخدمين محاولة العبث بسياسات الأمان التي تم إعدادها في أجهزتهم المحمولة.
- 7.7.4. يجب على المستخدمين التأكد من أنهم يستخدمون وحدات التخزين (USB) أو أقراص التخزين الصلبة الخارجية (external hard drives) المصرح بها رسميًا من قبل جامعة حفر الباطن.
- 8.7.4. يحظر على المستخدمين أخذ وحدات التخزين (USB) المُقدمة من قبل جامعة حفر الباطن إلى خارج جامعة حفر الباطن.
- 9.7.4. يجب على المستخدمين التأكد من فحص أجهزة الوسائط المحمولة الخاص بهم للكشف عن أي شفرة برمجية خبيثة.
- 10.7.4. يجب على المستخدمين إخطار نظام البلاغات الفنية فورًا في حال فقدان أو سرقة أجهزة الوسائط المحمولة الخاص بهم.
- 11.7.4. يجب على المستخدمين تقديم الأجهزة المحمولة التي بحوزتهم لأي مراجعة مطلوبة للتأكد من الالتزام بسياسات جامعة حفر الباطن.

8.4 استخدام الحواسيب المكتبية

- 1.8.4 يتحمل المستخدمون مسؤولية تأمين حواسيبهم المكتبية، ويتعين عليهم اتخاذ كافة التدابير اللازمة لضمان سلامة حواسيبهم.
- 2.8.4 يجب على المستخدمين قفل شاشة حواسيبهم قبل مغادرة مكاتبهم لمنع الآخرين من الوصول إلى أنظمتهم والوصول إلى المعلومات السرية.
- 3.8.4 يحظر على المستخدمين تخزين أي محتوى شخصي على الحواسيب المكتبية المُقدمة من جامعة حفر الباطن.
- 4.8.4 يجب على المستخدمين التعامل مع حواسيبهم المكتبية بعناية كبيرة وحمايتها من أي ضرر مقصود أو غير مقصود.
- 5.8.4 يجب على المستخدمين إخطار نظام البلاغات الفنية فورًا في حالة وجود أي مشكلة في حواسيبهم المكتبية.
- 6.8.4 يحظر على المستخدمين استخدام أي بطاقة تعريف أو كلمة مرور أو هوية خاصة بأي شخص آخر.
- 7.8.4 في حالة استلام المستخدم لمواد سرية عبر البريد الإلكتروني عن طريق الخطأ، أو إذا علم بوجود مواد سرية في جريدة عامة أو موقع إلكتروني، فيجب عليه إخطار نظام البلاغات الفنية في جامعة حفر الباطن.
- 8.8.4 يحظر على المستخدم استغلال نظام حاسوب المكتب للحصول على تصريح بالوصول إلى نظام حاسوب آخر.

9.4 إدارة كلمات المرور

1.9.4 يحظر على المستخدمين مشاركة كلمات المرور الخاصة بهم مع أي أحد داخل أو خارج جامعة حفر الباطن (يحظر حتى مشاركتها مع موظفي نظام البلاغات الفنية أو مديريهم) كما يجب تغيير كلمات المرور بصورة منتظمة أو عند وجود أي مؤشر على حدوث اختراق على أن يكون المستخدم مسؤولاً عن سرية كلمات المرور الخاصة به.

2.9.4 تحدد سياسة كلمات المرور الخصائص التالية للحفاظ عليها:

- الحد الأدنى لطول كلمة المرور
- تاريخ كلمة المرور
- تعقيد كلمة المرور
- تأمين الحساب في حالة حدوث محاولات متتالية غير ناجحة لتسجيل الدخول.

3.9.4 يجب على المستخدمين تغيير كلمات المرور المؤقتة عند أول تسجيل دخول.

4.9.4 لا يجوز للمستخدمين تضمين كلمات المرور في أي عملية تسجيل دخول آلية على سبيل المثال وحدات ماكرو إلخ.

5.9.4 يجب على المستخدمين الاحتفاظ بسميزات الوصول الحصرية لمرافق معالجة البيانات الخاصة بهم، وعدم السماح لأي أحد بالعمل بحسابهم.

6.9.4 يتحمل المستخدمون مسؤولية الأنشطة الناشئة من حساباتهم.

7.9.4 يحظر على المستخدم ترك كلمات المرور الخاصة بهم مكتوبة على مكاتبهم أو نسخها على شاشة الحاسوب أو تخزينها بأي شكل يسهل رؤيته من قبل الآخرين.

8.9.4 يجب على المستخدمين بذل العناية الواجبة أثناء استخدام كلمات مرورهم في وجود أشخاص حولهم ، أو في الأماكن العامة. وما إلى ذلك.

9.9.4 يجب على المستخدمين دائماً اختيار كلمات سهلة الحفظ ولكن لا يمكن تخمينها من قبل أي مهاجم. فلا يجوز استخدام كلمات المرور السهلة مثل الكلمات الموجودة في القاموس أو اسم الشخص أو تاريخ الميلاد أو شعارات أو أسماء حيوانات أليفة وغير ذلك.

10.9.4 يجب على المستخدم الالتزام دائماً بسياسة كلمات المرور (password policy) في جامعة حفر الباطن عند استخدام أنظمتها.

لمزيد من التفاصيل، يرجى الرجوع إلى سياسة كلمة المرور.

10.4 سياسة استخدام الانترنت

1.10.4 يحظر على المستخدمين توصيل أي مودم أو شبكة لاسلكية ببيئة جامعة حفر الباطن للوصول إلى أصول المعلومات في جامعة حفر الباطن.

2.10.4 يجب على المستخدمين التأكد من استخدام شبكات الانترنت جامعة حفر الباطن للأغراض الرسمية المخصصة لها فقط. ويجب عدم استخدام موارد الإنترنت لتسهيل الأعمال أو بيع المنتجات الشخصية أو الانخراط في أنشطة تجارية قد تسبب دعاية سلبية لجامعة حفر الباطن بخلاف المعلن عنه .

3.10.4 يجب تقييد الوصول إلى جميع مواقع البريد الإلكتروني على شبكة الإنترنت، ومواقع الدردشة، والموسيقى عبر الإنترنت، والألعاب، والترفيه، والقرصنة، وتطبيقات الوكيل (Proxy)، والشبكات الاجتماعية، ومشاركة الملفات من نظير إلى نظير (peer-to-peer) والمواقع الإباحية، واستخدام برامج المراسلة الفورية، وتنزيل صور ورق الحائط وشاشات التوقف وتطبيقات البرامج ومواقع الويب الأخرى غير المطلوبة لأغراض العمل.

4.10.4 يجب أن يدرك المستخدمون النهائيون أنه سيتم تسجيل الدخول إلى الإنترنت ومراقبته. تحتفظ الإدارة بالحق في فحص جميع الملفات المخزنة على أصول شبكتها أو المنقولة عبرها (بما في ذلك على سبيل المثال لا الحصر، وسائط التخزين المحلية والذاكرة وملفات البريد) بغرض التحقيق في الانتهاكات المشتبه بها للسياسات أو عدم الالتزام للوائح المحلية.

5.10.4 يجوز للمستخدمين محاولة التحقيق في الأنظمة الخارجية بحثًا عن نقاط الضعف الأمنية، أو اختراق الأنظمة الأخرى، أو امتلاك أو نقل البيانات بشكل غير قانوني، أو إرسال رسائل مسيئة.

6.10.4 يجب على المستخدمين استخدام شبكات الانترنت جامعة حفر الباطن لتنفيذ واجباتهم ومسؤولياتهم، وألا يحاولوا الوصول للإنترنت بطرق غير مصرح بها مثل: المودم الشخصي، وبطاقات الجوال ونقاط الوصول اللاسلكية غير المصرح بها وغير ذلك.

7.10.4 يجب على المستخدمين التأكد من اثبات هويتهم على النحو الصحيح للوصول إلى الانترنت عبر شبكات جامعة حفر الباطن .

8.10.4 يجب على المستخدمين التأكد من عدم وصولهم إلى الإنترنت بهوية مستخدم آخر.

9.10.4 يجب على المستخدمين التأكد من أنهم لا يسمحون لمستخدم آخر بالوصول إلى الإنترنت باستخدام هوياتهم.

10.10.4 يحظر على المستخدمين استخدام الانترنت في تنزيل وتوزيع برامج خبيثة على شبكة جامعة حفر الباطن وكذلك الأفلام والموسيقى وأي عناصر عمل أخرى غير ذات صلة.

11.10.4 لا يجوز للمستخدمين النهائيين تحميل أي نوع من المعلومات الرسمية على مواقع الويب الخارجية ما لم تأذن الإدارة بخلاف ذلك.

12.10.4 لا يجوز استخدام الانترنت للوصول إلى المواقع أو المحتويات المحظورة (مثل: المواقع الإباحية، المحتوي الإرهابي، الاحتيال، البرامج الخبيثة، المخدرات وغير ذلك).

13.10.4 يتحمل المستخدمون مسؤولية أي سوء استخدام للإنترنت ينشأ من حساباتهم.

11.4 استخدام البريد الإلكتروني

1.11.4 يحظر على المستخدمين إرسال أي بريد إلكتروني إلى جميع الموظفين، إلا من خلال الوصلة المسموح لها بإرسال بريد إلكتروني من هذا النوع هي إدارة العلاقات العامة.

2.11.4 يجب أن يكون المستخدمون على دراية بمستويات تصنيف السرية والالتزام به.

3.11.4 يجب على المستخدمين استخدام حسابات البريد الإلكتروني للأغراض المخصصة لها فقط.

4.11.4 يحظر على المستخدمين استخدام عنوان البريد الإلكتروني الرسمي للتواصل الشخصي.

5.11.4 يحظر على المستخدمين إرسال أو إعادة توجيه الفئات التالية من رسائل البريد الإلكتروني:

- رسائل البريد الإلكتروني التي تحتوي على عبارات تشهيرية أو إساءة وعنصرية أو عبارات مخلة.
- رسائل البريد الإلكتروني المُعاد توجيهها من قبل سلسلة من الأشخاص والتي تحتوي عادة على فيروسات أو نكت أو غير ذلك.
- رسائل البريد الإلكتروني التي تحتوي على أي وثائق أو برامج أو غيرها من المعلومات المحمية بحقوق الملكية الفكرية أو السرية أو لوائح الكشف.
- 6.11.4 يحظر على المستخدمين السماح لأي شخص آخر استخدام حساب البريد الإلكتروني الخاص بهم لأي نوع من المراسلات.

7.11.4 يجب على المستخدمين التأكد من أن جميع رسائل البريد الإلكتروني المرسلة من قبلهم موجهة إلى المستلمين المعنيين فقط.

8.11.4 يحظر على المستخدمين استخدام أي حسابات بريد إلكتروني خاصة بأي شخص آخر في أي نوع من أنواع المراسلات.

9.11.4 يجب على المستخدمين اتخاذ الحذر عند تقديم حسابات البريد الإلكتروني الخاصة بهم لمواقع خارجية مثل منصة المحادثات والقائمة البريدية وغير ذلك.

10.11.4 يجب على المستخدمين استخدام آلية توصيل الرسائل الافتراضية الخاصة بـ مايكروسوفت أوت لوك (MS Outlook) وأيضا منصة الويب للبريد الإلكتروني و البريد الإلكتروني من الهاتف المحمول طبقا لحاجة العمل.

11.11.4 يجب أن يدرك المستخدمون مسؤوليتهم تجاه إدارة أي نسخ محلية من صندوق البريد مخزنة على حواسيبهم المحمولة أو حواسيبهم المكتبية.

12.11.4 يجب على المستخدمين تأمين النسخة المحلية من صندوق البريد بكلمة مرور قوية.

13.11.4 يجب على المستخدم التأكد من تأمين مرفقات البريد الإلكتروني التي تحتوي على معلومات حساسة بكلمة مرور وإخطار المستلمين بهذه الكلمة عبر وسائل اتصالات أخرى مشفرة.

14.11.4 يجب على المستخدمين التأكد من عدم تنزيل أي مرفقات مشبوهة من البريد الإلكتروني وإبلاغ الدعم الفني للمستخدمين على الفور.

16.11.4 يتحمل المستخدمون مسؤولية أي سوء استخدام لمراسلات البريد الإلكتروني تنشأ من حساباتهم. في حالة إساءة استخدام البريد الإلكتروني، فسيتم حذف حساب البريد الإلكتروني الخاص بالمستخدم وتطبيق الإجراءات التأديبية اللازمة.

12.4 عناصر التحكم الأمنية المتعلقة بالاجتماعات والمؤتمرات

1.12.4 في حالة تواجد زائرين لحضور أي اجتماعات أو مؤتمرات داخل مباني جامعة حفر الباطن ، فيجب الالتزام بعناصر التحكم الأمنية لتأمين الأصول المحمية داخل هذه المباني قبل الفعالية وأثناءها وبعد انتهائها .

يجب اتباع الإرشادات التالية:

- 2.12.4 يجب أن تكون غرفة الاجتماعات / المؤتمرات غير مكشوفة ولا يمكن التنصت عليها.
- 3.12.4 يجب الحفاظ على عناصر التحكم في الوصول إلى غرفة الاجتماع أو المؤتمر قبل وأثناء الاجتماع وخلال أوقات الراحة. بمعنى أن يجلس أحد الأشخاص في الغرفة أثناء فترات الراحة للتأكد من عدم دخول أي شخص غير مصرح له إلى الغرفة.
- 4.12.4 يجب تأمين الأصول المحمية وغيرها من الأصول الحساسة أثناء فترات الراحة أو إغلاق الغرفة وحراستها.
- 5.12.4 يجب اتخاذ الإجراءات الأمنية اللازمة بعد الاجتماع أو المؤتمر للتخلص من الأصول المحمية أو الأصول الحساسة بشكل آمن، بالإضافة إلى اتخاذ تدابير نقل الأصول للأشخاص الذين يسافرون لحضور الاجتماع أو المؤتمر.

13.4 الأمن المادي

- 1.13.4 يجب على المستخدمين ارتداء بطاقات التعريف الخاص بهم بطريقة يسهل رؤيتها أثناء التواجد أو التحرك في أماكن عملهم والأماكن المحظورة.
- 2.13.4 يجب على المستخدمين تقديم بطاقات التعريف الخاصة بهم في حال طلبها من قبل موظفي الأمن داخل جامعة حفر الباطن .
- 3.13.4 يجب على المستخدمين إخطار الإدارة المعنية فوراً في حالة فقدان بطاقات التعريف الخاصة بهم.
- 4.13.4 يجب على المستخدمين الحصول على ترخيص من الجهات المعنية في حالة احتياجهم لإدخال حواسيبهم المحمولة الشخصية إلى أماكن العمل.
- 5.13.4 يجب أن يظهر المستخدمون حواسيبهم المحمولة الشخصية للاستقبال قبل إدخاله إلى مكان العمل.
- 6.13.4 يجب أن يظهر المستخدمون كافة أنواع المعدات الرسمية التي يأخذونها إلى داخل أو خارج مباني جامعة حفر الباطن .

7.13.4 يحظر على المستخدمين السماح بإتباع الموظفين الآخرين الذين لا يمتلكون صلاحية الوصول إلى المناطق المحظورة.

8.13.4 يحظر على المستخدمين التأثير على الظروف البيئية الخاصة بأي منطقة محظورة مثل مباني العمل، وغرف الخوادم، وغرفة الأرشفة، غرفة حفظ الملفات، وغرفة التخزين أو أي غرفة أخرى تحتوي على معدات.

9.13.4 يحظر على المستخدمين تناول أي مأكولات أو مشروبات في أي منطقة من المناطق المحظورة مثل وغرف الخوادم، وغرفة الأرشفة، غرفة حفظ الملفات، وغرفة التخزين أو أي غرفة أخرى تحتوي على معدات.

10.13.4 يحظر على المستخدمين التدخين داخل مباني جامعة حفر الباطن و استخدام الأماكن المخصصة لذلك خارج المبنى.

11.13.4 يجب على جميع المستخدمين المشاركة في تدريب الوقاية من الحريق للتأكد من معرفتهم لإجراءات السلامة البدنية في العمل.

14.4 الانتهاكات الأمنية

1.14.4 يقصد بالانتهاكات الأمنية أي اختراق للوائح أو المتطلبات أو الإجراءات أو الارشادات الأمنية سواء نتج عنها اختراق أو لا.

2.14.4 يجب إخطار إدارة نظم المعلومات فورًا عن أي انتهاك أمني مهما كان بسيطًا، حتى يتم تقييم الحادثة واتخاذ الإجراءات اللازمة.

3.14.4 لا يعفى إجراء الإبلاغ عن أي انتهاك أمني لموظفي جامعة حفر الباطن المعنيين من مسؤولياتهم.

4.14.4 تعد الأمور التالية من أمثلة الانتهاكات الأمنية:

- ترك ملفات سرية أو حاويات حفظ الملفات السرية مفتوحة أثناء ساعات العمل الرسمية أو بعدها.
- حفظ المستندات السرية في مكتب أو في خزانة أو درج أو منطقة غير مصرح بها.
- ترك المستندات السرية غير محمية على مكاتب أو طاوولات أو خزائن أو أي شيء آخر غير مؤمن سواء أثناء أو بعد ساعات العمل الرسمية.
- نسخ أو نقل أي مواد سرية دون الحصول على تصريح بذلك.
- نقل المعلومات السرية من مكان العمل للعمل عليها في المنزل.
- منح أي زائر أو جهة خارجية أو موظف أو أي شخص آخر صلاحية الوصول إلى المعلومات السرية دون التحقق من مستوى الترخيص أو مستوى حاجته للمعرفة.
- مناقشة المعلومات السرية في المكالمات الهاتفية، باستثناء الهواتف المصرح بها للمناقشات السرية.
- أن يحمل الشخص كلمات مرور الخزائن أو كلمات مرور الحاسوب معه، أو كتابتها على أي أوراق أو حفظها في درج مكتب أو غير ذلك من الأمور التي تهدد أمن أي خزانة أو حاسوب.
- عدم اتباع الإجراءات الصحيحة في التخلص من المواد السرية.
- أي شكل من أشكال الانتهاكات الأمنية نتيجة عدم الانتباه أو الإهمال أو عدم الاكتراث للإجراءات التأديبية.
- أخذ المعلومات السرية للمنزل عليها، أو أخذها أثناء السفر دون الحصول على تصريح بذلك.

- التدخل في المشاريع أو الأنشطة التي لا يملك الشخص (أو لم يعد يملك بعد) صلاحية معرفتها. ويتضمن ذلك طلب الحصول على مواد سرية من المكتبات المرجعية دون الحاجة الفعلية إلى ذلك، أو أي محاولة للوصول غير المصرح به إلى حواسيب أنظمة المعلومات أو قواعد البيانات.
- كشف المعلومات السرية عن عمد لأشخاص غير مصرح لهم لإظهار مدى أهمية الشخص.
- نسخ المعلومات السرية بطريقة تخفى تصنيفها، ويشير ذلك إلى نية الشخص في إساءة استخدام المعلومات السرية.
- عمل نسخ غير مصرح بها أو نسخ إضافية من المعلومات السرية. ويعد ذهاب الشخص إلى مكتب آخر لنسخ مواد سرية مع وجود معدات طباعة متاحة في منطقة عمله، بمثابة مؤشر على أنه غير مصرح له بنسخ تلك المستندات.

15.4 استخدام وسائل التواصل الاجتماعي

- 1.15.4 تهدف هذه السياسة إلى التأكد من أن جميع الموظفين يفهمون ويدركون واجباتهم ومسؤولياتهم عند استخدام وسائل التواصل الاجتماعي، بالإضافة إلى التحكم في المخاطر المتعلقة بهذا الاستخدام.
- 2.15.4 يجب أن يتأكد المستخدمين من توافق المعلومات التي ينشرونها على وسائل التواصل الاجتماعي مع سياسات أمن المعلومات.
- 3.15.4 لا يجوز للمستخدم وضع أي معلومات سرية أو معلومات متعلقة بالعمل في جامعة حفر الباطن في أي منصات وسائط اجتماعية.
- 4.15.4 لا يجوز للمستخدم وضع أي معلومات تتعلق بأدواره ومسؤولياته في جامعة حفر الباطن .
- 5.15.4 لا يجوز للمستخدم نشر أي معلومات حول أي من المعلومات والأسماء وقواعد البيانات المتعلقة بالتقنيات وما إلى ذلك والتي ترتبط بجامعة حفر الباطن .
- 6.15.4 لا يجوز للمستخدم نشر معلومات الاتصال مثل البريد الإلكتروني أو رقم الهاتف.
- 7.15.4 لا يجوز للمستخدم نشر أي صورة متعلقة بجامعة حفر الباطن على أي من منصات التواصل الاجتماعي. يحق فقط لقسم العلاقات العامة نشر الصور بعد الموافقة الرسمية والمعتمدة.
- 8.15.4 يجب على المستخدم الإبلاغ عن أي نشاط احتيالي ، على سبيل المثال لا الحصر ، انتحال الهوية أو التظاهر بأن لديه أدوارًا ومسؤوليات كاذبة و ذلك لإدارة الدعم الفني للمستخدم.
- 9.15.4 يجب أن يكون المستخدم على علم بأي محاولة هندسة اجتماعية مشبوهة والإبلاغ عنها.
- 10.15.4 لا يجوز للمستخدم قبول أي طلب تسويقي / تجاري. يجب إرسال أي طلب مباشرة إلى الإدارة ذات الصلة ، دون الموافقة على المناقشة.
- 11.15.4 لا يجوز للمستخدم التحدث ومقابلة الصحفيين الذين يحاولون الحصول على معلومات متعلقة بالأعمال أو سرية.
- 12.15.4 عند الاقتضاء، يجب على المستخدمين توجيه أي فرد يطلب معلومات عن جامعة حفر الباطن إلى الموقع الرسمي وقنوات التواصل الاجتماعي الخاصة به.

13.15.4. لا يجوز للمستخدم الوصول إلى محتوى غير لائق أثناء العمل، أو أثناء استخدام موارد جامعة حفر الباطن.

14.15.4. لا يجوز للمستخدم النهائي مناقشة أي معلومات حساسة ما لم تتم الموافقة عليها من خلال العملية الرسمية.

15.15.4. يحظر استخدام الشعارات أو العلامات التجارية الخاصة بجامعة حفر الباطن إلا بعد الحصول على تصريح بذلك من خلال الموافقة الرسمية.

16.15.4. يحتفظ جامعة حفر الباطن بالحق في طلب حظر موضوعات معينة، و حذف منشورات معينة ، وإزالة التعليقات غير الملائمة. يجب على جميع الموظفين أو موظفي الأطراف الخارجية استخدام التعليمات التالية عند نشر المعلومات على وسائل التواصل الاجتماعي:

- يجب معرفة واتباع جميع إرشادات سياسة الخصوصية والسرية في جامعة حفر الباطن .
- لا يجوز الكشف أو استخدام أي معلومات سرية أو مملوكة لجامعة حفر الباطن ، أو أي معلومات مملوكة لأي شخص أو شركة أخرى. على سبيل المثال، يجب الحصول على إذن من الشخص قبل نشر صورته على شبكة التواصل الاجتماعي، أو نشر محادثة خاصة على أي مدونة.
- لا يجوز الاقتباس من أو الإشارة إلى العملاء، أو الزملاء، أو الموردين دون الحصول على إذن كتابي منهم.
- يجب التحدث بصيغة المتكلم عند الانخراط في اتصالات ووسائل التواصل الاجتماعي الشخصية. يجب على الموظفين توضيح أنه يتحدث نيابة عن نفسه وليس نيابة عن جامعة حفر الباطن .
- لا يجوز استخدام الإهانات العرقية أو الشخصية أو الألفاظ البذيئة أو الانخراط في أي سلوك غير مقبول في أماكن عمل جامعة حفر الباطن . يجب إظهار الاعتبار المناسب لخصوصية الآخرين وللمواضيع غير اللائقة أو التحريضية.
- لا يجوز تنفيذ أعمال سرية مع عميل أو شريك عبر حسابات التواصل الاجتماعي الشخصية الخاصة به أو بأي أحد آخر.
- لا يجوز التسجيل في أي حساب باستخدام اسم جامعة حفر الباطن أو أي علامة تجارية أخرى سواء كانت مسجلة أو غير مسجلة. لا يجوز التسجيل في أي حساب باستخدام اسم جامعة حفر الباطن أو أي علامة تجارية أخرى سواء كانت مسجلة أو غير مسجلة.

17.15.4 يجب على جميع الموظفين ضمان الاحترام الدائم تجاه:

- جامعة حفر الباطن
 - أعضاء فريق العمل الآخرين.
 - الشركات والمنافسون والجهات الخارجية.
- 18.15.4 يجب أن يدرك الموظفون أن أي تعليقات غير محترمة لما ورد أعلاه قد يُنظر إليها على أنها تشهيرية وقد تؤدي إلى اتخاذ إجراءات تأديبية أو إنهاء العقد.

19.15.4. يجب على أي موظف يدرك وجود أي نشاط مكروه في شبكات الاجتماعية إبلاغ إدارة جامعة حفر الباطن في أقرب وقت ممكن.

تنفيذ السياسة والالتزام بها

يعد الالتزام بهذه السياسة إلزاميًا، ويجب على مديري إدارات جامعة حفر الباطن التأكد من الالتزام المستمر لتلك السياسة داخل إداراتهم. يخضع الالتزام لبيانات هذه السياسة لمراجعة دورية.

يُعد انتهاك هذه السياسة بمثابة مخالفة أمنية تعطي جامعة حفر الباطن الحق في اتخاذ الإجراءات التأديبية والقانونية اللازمة والتي قد تصل إلى إنهاء الخدمة أو علاقة العمل. تُحدد الإجراءات التأديبية بناءً على شدة الانتهاك الذي تبينه التحقيقات.

معيار الاستثناءات المتعلقة بهذه السياسة

الغرض من هذه السياسة هو تلبية متطلبات الأمن السيبراني. لذا فعند الحاجة، يجب تقديم الاستثناءات المتعلقة بهذه السياسة رسميًا إلى اللجنة الإشرافية الأمن السيبراني، مع إدراج السبب وراء هذه الاستثناءات والمزايا المترتبة عليها.

تبلغ فترة الاستثناءات المتعلقة بهذه السياسة 4 أشهر كحد أقصى، ويجب إعادة تقييمها والموافقة عليها، إذا لزم الأمر، لمدة أقصاها ثلاث فترات متتالية. لا يجوز تقديم الاستثناءات لأكثر من ثلاث فترات متتالية.

مراجع ISO27001

- بند أ.8.1.3 الاستخدام المقبول للأصول
- بند أ.11.2.9 سياسة المكتب النظيف والشاشة النظيفة.

مراجع إطار الهيئة الوطنية للأمن السيبراني

الضوابط الأساسية للأمن السيبراني (ECC – 2 : 2024)

- 1.2 إدارة الأصول

السياسات ذات الصلة

وتشمل جميع سياسات الأمن السيبراني

مراجعة الوثيقة

- سيتم مراجعة هذه الوثيقة بشكل دوري (سنوي) ليتم ضمان تحديثها بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
- يستلزم التقدم التقني والتغيرات في متطلبات الأعمال إجراء مراجعة دورية للسياسات. ومن ثم، يجوز تعديل هذه السياسة لتعكس التغييرات أو تُحدد المتطلبات الجديدة أو المُعدلة.
- يتطلب إجراء أي تغيير في السياسة الحصول على موافقة من اللجنة الإشرافية للأمن السيبراني.

التعريفات

المصطلح	التعريف
تحمل المسؤولية	مبدأ أمني يشير إلى أنه يجب توفير إمكانية تحديد هوية الأشخاص، وأنهم يتحملون مسؤولية أفعالهم.
الأصول	الأصل هو أي شيء ذو قيمة بالنسبة للمؤسسة.
التوفر	إمكانية الوصول واستخدام الممتلكات عند الطلب من قبل أي جهة معتمدة.
السرية	المعلومات غير المتاحة والتي لا يجوز الكشف عنها لأي أشخاص أو هيئات أو عمليات غير مرخص لهم.
أمن المعلومات	حماية سرية وسلامة وتوافر المعلومات، بالإضافة إلى بعض الخصائص الأخرى التي يمكن إدراجها مثل الموثوقية والخضوع للمساءلة وعدم التنصل والمصادقية.
السلامة	الحفاظ على دقة وتكامل المعلومات.
جامعة حفر الباطن	جامعة حفر الباطن
السياسة	خطة عمل لتوجيه القرارات والإجراءات. ربما ينطبق هذا المصطلح على الهيئات الحكومية ومؤسسات القطاع الخاص والمجموعات والأفراد. تتضمن السياسة تحديد بدائل مختلفة، مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس النتائج المترتبة على كل منهما.
الجهات الخارجية	أي شخص أو جهة أو هيئة مستقلة عن جامعة حفر الباطن، والتي يتطلب التعامل مع أي منهم إجراءات تعاقدية و يشمل ذلك الموردين ، البائعين ، المتعاقدين ، الاستشاريين و شركاء الأعمال، إلخ...
المعلومات الحساسة	أي معلومة عن جامعة حفر الباطن ينطبق عليها أحد تصنيفات السرية التالية طبقاً لإرشادات مكتب إدارة البيانات • سري للغاية • سري • مقيد