

عمادة تقنية المعلومات
والتعليم الإلكتروني
Deanship of Information
Technology & E-Learning



جامعة حائل
University of Hail

رؤية
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA



سياسة أمن الموارد البشرية

بجامعة حائل

م2023/2022

سَمِعْنَا وَأَطَعْنَا
اللَّهُمَّ صَلِّ عَلَى مُحَمَّدٍ

سياسة أمن الموارد البشرية بجامعة حائل

الصفحات	المحتويات
4	معلومات ذات ملكية فكرية
الرقابة على الوثيقة	
5	معلومات عن الوثيقة
5	الإعداد والتحديث
5	قائمة التوزيع
5	الاعتماد
نظرة عامة على السياسة	
6	الغرض
6	النطاق
7	المصطلحات والتعريفات
7	التغيير والمراجعة والتحديث
8	النفاذ والامتثال
8	الاستثناءات
9	الأدوار والمسؤوليات (مصفوفة المهام RACI)
10	الوثائق ذات الصلة
10	الملكية
بيانات السياسة	
11	التحري
12	شروط وأحكام التوظيف
12	المسؤوليات الإدارية
13	الوعي بأمن المعلومات والتثقيف بها والتدريب عليها
13	العملية التأديبية
20	إنهاء الخدمة أو تغيير المسؤوليات المتعلقة بالوظيفة

Deanship of Information
Technology & E-Learning



عمادة تقنية المعلومات
والتعليم الإلكتروني

معلومات ذات ملكية فكرية:

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة تقنية المعلومات والتعليم الإلكتروني في جامعة حائل. وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة تقنية المعلومات والتعليم الإلكتروني. جميع الحقوق محفوظة لعمادة تقنية المعلومات والتعليم الإلكتروني.

الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة أمن الموارد البشرية	عام	2.0	عام

الإعداد والتحديث

الإصدار	المؤلف / المؤلفون	تاريخ الإصدار	التغييرات
0.1			إعداد
0.2			مراجعة
0.3			تحديث
1.0			مسودة
1.1			
1.2			
2.0			

قائمة التوزيع

المستفيد	#
إدارة الشؤون القانونية	1
الموقع الإلكتروني للجامعة	2
قسم ضمان الجودة بالعمادة	3
قسم إدارة أمن المعلومات بالعمادة	4

الاعتماد

الاسم	الصفة	التاريخ	التوقيع
د. خالد بن عبدالعزيز العتيبي	عميد تقنية المعلومات والتعليم الإلكتروني		

نظرة عامة على السياسة:

يستعرض هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها وتعريف مصطلحاتها وتعريفها، وتغييرها، ومراجعتها، وتحديثها، وإنفاذها والامتثال لها، والأدوار والمسؤوليات، واستثناءاتها، والوثائق ذات الصلة بالإضافة الملكية الوثيقة.

الغرض:

الغرض الرئيسي من سياسة أمن الموارد البشرية هو:

ضمان أن منسوبي جامعة حائل والمتعاقدين معها يدركون مسؤولياتهم ويلتزمون الأدوار التي تسند إليهم، والتأكد من أن المنسويين والمتعاقدين على دراية بمسؤولياتهم المتعلقة بأمن المعلومات والوفاء بها، وحماية مصالح الجامعة الأخرى في إطار عملية التغيير أو إنهاء العمل مل .

النطاق:

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع موارد جامعة حائل بكل مستويات حساسيتها، بما فيها:

- جميع الموظفين بدوام كامل وبدوام جزئي والموظفين المؤقتين الذين يعملون لدى جامعة حائل أو يعملون لصالحها أو بالنيابة عنها.
- الطلاب الذين يدرسون في جامعة حائل.
- المقاولون والاستشاريون الذين يعملون لصالح جامعة حائل أو نيابة عنها.
- جميع الأفراد والجماعات الأخرى الذين تم منحهم إمكانية الوصول إلى أنظمة تقنية المعلومات والتعليم الإلكتروني في جامعة حائل.

تغطي هذه السياسة جميع أصول المعلومات المحددة في وثيقة نطاق تقييم المخاطر وسيتم استخدامها كأساس لإدارة أمن المعلومات.

المصطلحات والتعريفات:

• يوفر الجدول تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى ضرورة القدرة على تحديد هوية الأفراد وتحملهم مسؤولية أفعالهم.
الأصول	المعلومات التي تعتبر ذات قيمة بالنسبة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفر	الحالة التي في ظلها تكون جهة مصرح لها قادرة على الوصول إلى أحد الأصول أو إحدى الخدمات واستخدامها عند الطلب.
السرية	عدم توفر اصل من الأصول أو خدمة من الخدمات أو الكشف عنها لأفراد أو جهات أو عمليات غير مصرح بها.
الرقابة	وسيلة لإدارة المخاطر تشمل السياسات والإجراءات والإرشادات التي يمكن أن تكون ذات طبيعة إدارية أو تقنية أو إدارية أو قانونية.
الإرشاد	وصف لمتطلبات تحقيق الأهداف المحددة في السياسات وطريقة القيام بهذه المتطلبات.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفرها يشمل أمن المعلومات استخدام خصائص أخرى تتعلق بها مثل التحقق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول طوال دورة حياتها بأكملها والتأكد من دقتها وتناسقها.
المالك (المصاحب)	أي شخص أو مجموعة من الأشخاص تم تحديدهم من قبل الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوافرها وسلامتها. وقد يتغير المالك أثناء دورة حياة الأصل.
السياسة	خطة عمل يسترشد بها عند اتخاذ القرارات والإجراءات. تتضمن عملية السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس التأثير الذي ستحدثه.
الخطر	مزيج من عواقب الحدث واحتمالات حدوثها (بما في ذلك التغييرات في الظروف) واحتمال حدوثها.
الفحص	عملية التحقق من الوقائع المتعلقة بهويات الأفراد وأوراقهم المهنية ووظائفهم ومهاراتهم السابقة.
النظام	جهاز أو نظام مترابط أو أنظمة فرعية من المعدات تستخدم في الحصول على البيانات أو تخزينها أو معالجتها أو إدارتها أو التحكم فيها أو عرضها أو تعديلها أو تبادلها أو نقلها أو استقبالها، بما في ذلك برامج الحاسب آلي والبرامج الثابتة والأجهزة.

التغيير، المراجعة والتحديث:

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. ولا يجري تغييرات في هذه السياسة إلا ضابط أمن المعلومات ويجب أن تعتمد الإدارة هذه التغييرات كما يجب أن يظل سجل التغيير محدثاً بحيث يتم تحديثه بمجرد إجراء أي تغيير.

الإفزاز والامثال:

يعد الالزام بهذه السياسة أمر واجبا ويجب التأكد منه بشكل دوري من قبل ضابط أمن المعلومات. كما يجب على جميع وحدات جامعة حائل (من عمادة، وإدارات، وكليات، وأقسام ومراكز) ضمان مراقبة الامثال المستمر في نطاق وحداتهم.

وفي حالة تجاهل أو انتهاك توجيهات أمن المعلومات، يمكن أن تتضرر بيئة الجامعة (على سبيل المثال، تفقد الجامعة الثقة فيها وتفقد سمعتها أو تحدث اضطرابات تشغيلية أو مخالفات قانونية فيها)، وهذا يجعل الأشخاص الذين ارتكبوا تلك الأخطاء مسؤولين عنها مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة بل يمكن أن يخضعوا للتحقيقات القانونية).

يجب معاملة الموظفين الذين يشتهب في انتهاكهم للأوامر الأمنية معاملة صحيحة وعادلة (كأن تتخذ ضدهم إجراءات

تأديبية). ويجب إبلاغ إدارة الموارد البشرية لمعالجة انتهاكات السياسة والتعامل مع هذا الأمر بالطريقة المناسبة.

الاستثناءات:

يجب أن ينظر أمن المعلومات في الاستثناءات المطلوبة على أساس فردي، ويجب أن يشفع كل طلب استثناء من الامثال لهذه السياسة بالمبررات المنطقية التي دعت لتقديمه حيث يوافق ضابط أمن المعلومات على هذا الاستثناء وتعتمده عمادة تقنية المعلومات والتعليم الإلكتروني. يجب أن يشمل كل طلب استثناء المبررات والمزايا التي تنسب إليه.

تبلغ فترة الاستثناء من السياسة أربعة أشهر كحد أقصى، ويجوز تمديد الاستثناء لمدة أقصاها ثلاثة فترات متتالية وذلك بعد إعادة تقييمه واعتماده. ولن يجدد أي استثناء لأكثر من ثلاث فترات متتالية.

الأدوار والمسؤوليات (مصفوفة المهام RACI):

يوضح الجدول مصفوفة المهام (RACI) التي تحدد الشخص المسائل أو المسؤول أو الشخص الذي تتم استشارته أو إبلاغه بكل مهمة يجب تنفيذها، وتشتمل هذه السياسة على أدوار تطلع بها الأطراف التالية على التوالي: عمادة تقنية المعلومات والتعليم الإلكتروني، وموظف أمن المعلومات، وإدارة الموارد البشرية أو الوحدة الإدارية والإدارة القانونية، والوكالة المعنية بالاستقطاب لأجل التوظيف، ومدير الإدارة والمستخدم الموظف والمتعاقد.

المستخدم	مدير الإدارة	وكالة الاستقطاب الوظيفي	الإدارة القانونية	الموارد البشرية أو الوحدات الإدارية	ضابط أمن المعلومات	تقنية المعلومات	الاسم المسؤوليات
I			C,I	R,I	R,A	R	إدارة التدريب الأمني وبرامج التوعية لموظفي الجامعة بالتنسيق مع إدارة شؤون الموظفين.
I			R		C	C	تقديم المشورة القانونية المتخصصة اللازمة للإدارات الأخرى لتقديم الخدمات بطريقة متوافقة تماما مع القوانين واللوائح الحالية.
				R,A	C	C,I	إعداد شاشة خاصة بالموظفين في جميع مراحل التوظيف.
I			C	R,A	C	C,I	تحديد وتنفيذ الإجراء التأديبي المناسب عندما يكون هناك انتهاك لسياسة أمن المعلومات الخاصة بجامعة حائل.
		R,A		C,I	C	I	التمسك بسياسة أمن الموظفين المعمول بها في الجامعة أثناء عملية التوظيف (على سبيل المثال، فحص المرشحين للوظائف والتحقق من المعلومات المتعلقة بهم).
I				R,A	C	C	تبلغ هذه السياسة إلى جميع موظفي الجامعة الجدد والمتعاقدين معها للتأكد من استيعابهم لسياسات أمن المعلومات ومتطلباتها والمسؤوليات المترتبة عليها.
R,A,I				C	C	C	الالتزام بسياسات أمن المعلومات والإرشادات والإجراءات المتعلقة بحماية المعلومات.
R				C	C	I	توقيع تعهد بعدم الإفصاح عن ما تضمنته هذه السياسة من أحكام.
I				R,A	C	C,I	إعداد وصف وظيفي للعاملين في الجامعة والتأكد من أن الوصف الوظيفي للموظف الجديد يشتمل على الالتزام بسياسة أمن المعلومات الخاصة بجامعة حائل.
		C,I		R,A	C	C	التعاون مع الأطراف المشاركة و / أو إبلاغها في حالة حدوث تغييرات في الواجبات أو إنهاء خدمة الموظف.
		C,I		R,A	C	C	التأكد من أن الموظف المستقيل أو المنتوية مدة خدمته قد أعاد جميع الأصول الخاصة بالجامعة التي في عهده قبل إكمال عملية إنهاء الخدمة.
I				C	C	R,A	إلغاء حقوق الوصول المنطقية والمادية للأصول عند إنهاء خدمة الموظف أو تغييره.
	R,A			I	C	C	دعم الموظفين الخاضعين للإشراف وضمان قيامهم بتطبيق الأمن وفقا للسياسة أمن المعلومات الخاصة بجامعة حائل.
I				R	R,A	C	تخطيط وإعداد وتقديم دورات التوعية بأمن المعلومات لموظفي الجامعة.

اتصف مصفوفة راعي (RACI) الخاصة بتحديد المسؤوليات والأدوار المختلفة التي يشارك بها أعضاء الفريق في إنجاز مهام العمل، وهي مفيدة بشكل خاص في توضيح الأدوار والمسؤوليات عند تنفيذ عمليات متعدد فيها الوظائف أو الإدارات، يرمز الحرف (R) إلى الموظف الذي ينفذ مهمة من المهام، أما الحرف (A) فيرمز للشخص المسؤول (أو جهة الاعتماد) حيث يوقع هذا الشخص أو يعتمد المهمة المناطة إلى الموظف) * (R أما الحرف (C) فيرمز إلى المستشار الذي يقدم رأياً حول ما هو مراد تنفيذه، ويرمز الحرف (I) إلى الشخص الذي يكون على علم ودراية بالمهمة وهو الذي تصله أحدث المعلومات عن سير المهمة.

الوثائق ذات الصلة:

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه السياسة:

- سياسة أمن المعلومات.
- سياسة أمن الموارد البشرية.
- سياسة إدارة حوادث أمن المعلومات.
- سياسة الامتثال.

الملكية:

هذه الوثيقة مملوكة وتحافظ عليها عمادة تقنية المعلومات والتعليم الإلكتروني بجامعة حائل وهي التي تحافظ عليها.



بيانات السياسة

تقدم الأجزاء الفرعية التالية بيانات السياسة في ستة جوانب رئيسية:

- التحري
- شروط وأحكام التوظيف
- المسؤوليات الإدارية
- المعلومات والتثقيف بها والتدريب عليها.
- العملية التأديبية
- إنهاء الخدمة أو تغيير مسؤوليات الوظيفة.

التحري:

1. تضع إدارة الموارد البشرية أو الوحدة الإدارية المعنية عملية رسمية تحدد بموجبها الخطوات والإجراءات المطلوبة للتوظيف لجميع منسوبي الجامعة ولاستقلالهم من العمل وإنهاء خدمتهم.
2. يجب على إدارة الموارد البشرية أو الوحدة الإدارية المعنية أو الجهات الخارجية المناسبة إجراء فحص «مناسب للتحقق من المعلومات التي تمثل خلفيات لجميع المرشحين للعمل أو تشير لوضع المقاولين أو حالة المستخدم الذي يمثل طرف ثالثاً. ويجب أن تأخذ عملية الفحص في الاعتبار مستوى الثقة والمسؤولية المرتبطة بالوظيفة وما تسمح به قوانين العمل السعودية ويتمثل ذلك فيما يلي:
 - أ. احتياجات العمل في جامعة حائل، والمتطلبات القانونية والتنظيمية ذات الصلة.
 - ب. تصنيف وحساسية المعلومات والنظام والخدمات والبنية التحتية التي يمكن الوصول إليها والمخاطر المتوقعة.
 - ج. الخصوصية وحماية المعلومات الشخصية وغيرها من تشريعات العمل ذات الصلة.
 - د. التأكد من الأشياء التالية ومراجعتها عندما يقتضي الأمر:
 - إثبات الهوية الشخصية (على سبيل المثال، الهوية الوطنية، جواز السفر).
 - إثبات المؤهلات الأكاديمية (على سبيل المثال، الشهادات عن طريق الحصول على الوثائق الأصلية أو من خلال التحقق المباشر مع المؤسسة ذات الصلة.
 - دليل على الخبرة العملية (على سبيل المثال، السيرة الذاتية والجهات التي يمكن الرجوع إليها).
 - التحقق من اثنين من الجهات المرجعية في مكان العمل.
 - سجل الصحيفة الجنائية.
3. على وكالات التوظيف أو الأطراف الثالثة التي توفر مقاولين واستشاريين مباشرة إلى جامعة حائل أن تقوم على الأقل بنفس المستوى من اختبارات التحقق من خلفية الموظفين كما هو موضح في سياسة أمن الموارد البشرية (أي كجزء من مسؤوليات الوكالة).

شروط وأحكام التوظيف:

١. يجب توضيح المسؤوليات القانونية وحقوق الموظف المتعلقة بالعمل في جامعة حائل لجميع موظفي الجامعة في بداية توظيفهم ويجب أن يتم تحديد هذه المسؤوليات والحقوق بوضوح في الاتفاقية الموقعة بين الطرفين.
٢. يجب على جميع موظفي جامعة حائل توقيع اتفاقية مناسبة تتعلق بالسرية عند مباشرتهم أعمالهم. تتطلب هذه الاتفاقية من الموظف الامتثال لجميع سياسات وإجراءات أمن المعلومات المعمول بها في جامعة حائل.
٣. يطلب من الموظفين المتعاقدين أو الوكالة التي تزود الجامعة بالموظفين الذين يزورون المناطق الحساسة (مثل مركز البيانات الرئيسي وغرف الخادم) توقيع اتفاقية السرية على النحو المطلوب.
٤. يجب أن تتضمن شروط وأحكام التوظيف كل مسؤولية للمستخدم تجاه أمن المعلومات.

المسؤوليات الإدارية:

١. يتعين على جميع مديري الإدارات ورؤساء الأقسام مطالبة جميع الموظفين، الذين يعملون تحت إشرافهم تطبيق متطلبات الأمن وفقا لسياسات وإجراءات أمن المعلومات الخاصة بجامعة حائل.
٢. يجب على جميع مديري الأقسام والوحدات الإدارية في الجامعة التأكد من أن الموظفين يتحلون بما يلي:
 - أ. الإلمام المناسب بأدوارهم ومسؤولياتهم تجاه أمن المعلومات الخاصة بهم.
 - ب. الحماس للوفاء بسياسات أمن المعلومات الخاصة بجامعة حائل.
 - ج. الاستمرار في الحصول على المهارات والمؤهلات المناسبة.
 - د. حضور دورات تثقيفية منتظمة (خاصة بجوانب أمن المعلومات).
٣. يجب أن يكون الإداريون ملمين بالظروف الشخصية المحيطة بموظفيهم، وأن يراقبوا أي تغيير سلوكي قد يؤدي إلى اختراق أمني أو مخالفة أمنية.
٤. على الإداريين التأكد من أن إجازات الموظفين وغيابهم عن العمل لا يؤثر على توفر وأداء الخدمة في حائل. وعندما يتقدم الموظف بطلب للحصول على إجازة، عليه أن يأخذ في الاعتبار ما يلي:
 - أ. إرسال طلب الإجازة قبل وقت كاف للمعالجة.
 - ب. إعداد قائمة بالواجبات والأنشطة المرتقب القيام بها في فترة الإجازة وذكر اسم الموظف أو أسماء الموظفين المسؤولين عن أداء هذه الواجبات والأنشطة خلال تلك الفترة.
 - ج. يجب على الموظف التأكد من استمرار العمل أثناء غيابه.

الوعي بأمن المعلومات والتثقيف بها والتدريب عليها:

1. يجب توفير الوعي المناسب بأمن المعلومات وتدريب موظفي الجامعة على هذا الأمر وتثقيفهم به، مع توضيح مسؤولياتهم المتعلقة بسياسات وإجراءات أمن المعلومات الخاصة بالجامعة وجميع الالتزامات ذات الصلة المحددة في الوصف الوظيفي. قد يشمل الوعي الأمني، على سبيل المثال لا الحصر:
 - أ. عملية تعريفية رسمية تتضمن التدريب الأمني، قبل منح الوصول إلى شبكة وأنظمة جامعة حائل.
 - ب. التدريب المستمر على متطلبات الرقابة الأمنية والمسؤوليات القانونية التنظيمية وإجراءات أمن المعلومات المقبولة عموماً، بما يتناسب مع أدوار الموظفين ومسؤولياتهم.
2. يجب أن يشمل الوعي بأمن المعلومات الجوانب العامة مثل:
 - أ. التزام إدارة جامعة حائل بأهداف أمن المعلومات.
 - ب. الإجراءات الأساسية لأمن المعلومات (مثل الإبلاغ عن الحوادث المتعلقة بأمن المعلومات ومعايير الأمن (مثل تأمين كلمة المرور وحماية استخدام الأصول وعناصر التحكم في مكافحة الفيروسات والمكاتب النظيفة والمرتبطة الأوضاع).
 - ج. المساءلة الشخصية والمسؤوليات تجاه حماية أصول جامعة حائل.
3. يقوم ضابط أمن المعلومات بالتنسيق مع إدارة عمادة تقنية المعلومات والتعليم الإلكتروني وشؤون الموظفين بما يلي:
 - أ. إعداد برنامج سنوي للتوعية بأمن المعلومات وخطة التدريب، تفي بهذا الغرض.
 - ب. إصدار مواد للتوعية (على سبيل المثال، مطبوعات المعلومات أو اتصالات البريد الإلكتروني من أجل إبقاء جميع موظفي جامعة حائل على دراية بأدوارهم ومسؤولياتهم المتعلقة بأمن المعلومات.
4. يجب على الإدارة تخصيص وقت عمل كاف لموظفي الجامعة لكي يطلعوا على سياسات وإجراءات أمن المعلومات الخاصة بالجامعة وطرق إدارة الأعمال ذات الصلة.
5. يجب على كل موظف في جامعة حائل حضور جلسة للتوعية بأمن المعلومات في غضون ثلاثة أشهر من تاريخ التحاقه بالوظيفة. ويجب على كل موظف أن يوقع على ورقة تؤكد بأنه حضر هذه الجلسات، وفهم المواد المقدمة خلالها، وأتيحت له الفرصة لطرح الأسئلة التي تختمر في ذهنه، والموافقة على أداء عمله وفقاً لسياسات وإجراءات أمن معلومات الجامعة.

العملية التأديبية:

١. يجب أن توفر العملية التأديبية استجابة تدريبية تراعي العوامل التالية:
 - أ. طبيعة وشدة الخرق الأمني الذي وقع فيه الموظف أو المتعاقد.
 - ب. أثر الخرق على العمل.
 - ج. مدى تكرار الجريمة من عدمه.
 - د. خضوع المخالف لتدريب مناسب من عدمه.
 - هـ. التشريعات ذات الصلة.
٢. يتخذ إجراء تأديبي رسمي وفقا لسياسات وإجراءات الجامعة والإرشادات والمذكرات الموجهة للعاملين فيها.
٣. لا يجوز استخدام المعلومات الخاصة بجامعة دائل ولا بنيتها التحتية (مثل الشبكات والأنظمة والخدمات لأغراض أخرى غير احتياجات العمل في الجامعة، ويجب التعامل مع أي أنشطة احتيالية يتم اكتشافها وفقا للإجراءات التأديبية الخاصة بالعاملين في الجامعة.

إنهاء الخدمة أو تغيير المسؤوليات المتعلقة بالوظيفة:

١. يجب تحديد مسؤوليات وممارسات إنهاء الخدمة أو تغيير الوظيفة بوضوح. وقد يشمل ذلك، على سبيل المثال لا الحصر:
 - أ. عمليات الإنهاء التي تضمن حجر الوصول إلى جميع مصادر المعلومات.
 - ب. تغيير المسؤوليات والواجبات داخل جامعة دائل إثر إجراءات ومعالجات تتخذها كإنهاء العمل على الوظيفة القديمة وإعادة التوظيف (والتسكين في وظيفة جديدة)، باستخدام ضوابط سياسة النقل التي تحكم تلك العمليات ما لم يرد خلاف ذلك.
 - ج. العمليات التي تضمن إطلاع الموظفين بشكل مناسب على الحالة المتغيرة للشخص، وأي مسؤوليات ما بعد التوظيف محددة في شروط وأحكام العمل، أو عقد المقاول أو الطرف الثالث.

٢. على إدارة الموارد البشرية (أو الوحدة الإدارية المعنية بالتعاون مع المشرفين على الموظف إخطار عمادة تقنية المعلومات والتعليم الإلكتروني على الفور بنقل الموظف أو تغيير الواجبات المكلف بها، بحيث يتم اتخاذ جميع التدابير التي تتعلق بإلغاء أو تغيير حقوق الوصول المنطقية و / أو المادية للأصول.

٣. في حالة إنهاء خدمة الموظف، يتم النظر فيما يلي:

- أ. إعفاء الموظف من جميع الواجبات ذات الصلة بجامعة حائل وإنهاء جميع الامتيازات المتعلقة بالعمل وقت إنهاء الخدمة.
- ب. استعادة جميع الممتلكات والمعلومات التي في عهدة الموظف المعني وتخص الوحدة الإدارية التابعة للجامعة قبل مغادرة الموظف المباني جامعة حائل.
- ج. إخطار جميع المسؤولين الذين يتعاملون مع الحسابات التي يستخدمها الموظف بمجرد معرفة أن خدمته قد أنهيت.





عمادة تقنية المعلومات
والتعليم الإلكتروني
Deanship of Information
Technology & E-Learning



رؤية VISION
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA