2026

جامعة الأمير سطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY

سجل السياسات في جامعة الأمير سطام بن عبد العزيز

رمز الوثيقة	TP-GOV-L-000-001	
الإصدار	1,0	
تاريخ الإصدار	01/04/2026	
أنشئت بواسطة	مكتب الحوكمة والامتثال المؤسسي	
و افق عليها	مدير مكتب الحوكمة والامتثال المؤسسي	محمد سعد عياد الحربي
مستوى الخصوصية	☐ عام ☒ داخلي ☐ محظور ☐ سري	
عدد الصفحات	٢٥	

معلومات الوثيقة	
معد الوثيقة	محمد سعد عياد الحربي
مُعدة إلى	مكتب الحوكمة والامتثال المؤسسي
تاريخ الإعداد	2026/04/01
نوع الوثيقة	سجل السياسات في جامعة الأمير سطام بن عبد العزيز

تواريخ إصدارات ومراجعات الوثيقة:

الإصدار	تاريخ الإصدار	معد الوثيقة	التغييرات بالوثيقة
1.0	2026/04/01		نسخة أولية
1.1			

الاعتماد:

	الاسم	الوظيفة	التاريخ
اعتمدت بواسطة			2026/00/00
اعتمدت بواسطة			2026/00/00

أولًا: مقدمة

أنشئ مكتب الحوكمة والامتثال المؤسسي وتشكيل اللجنة المشرفة على أعمال المكتب بقرار رئيس الجامعة رقم ١٤٧١٧٩٢٣ وتاريخ ١٤٤٧/٠٥/١٨هـ لرفع مستويات النضج المؤسسي وتعزيز الثقة المؤسسية بما يدعم الحصول على الاعتمادات الأكاديمية والمؤسسية ورفع تصنيفات الجامعة في جميع المرجعيات المحلية والدولية.

سجل السياسات في جامعة الأمير سطام بن عبد العزيز

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
١	TP-GOV-PO-001	سياسة الإفصاح وتعارض المصالح	تبين هذه السياسة الحالات التي يجب فيها الإفصاح عن حالات تعارض المصالح	٢٠٢٦	مكتب الحوكمة والامتثال المؤسسي	جميع منسوبي الجامعة والمتعاملين والمستفيدين		سارية	•
٢	TP-GOV-PO-002	سياسة الإبلاغ عن المخالفات	قواعد عامة للإبلاغ عن المخالفات الإدارية والمالية والتظلمات	2022	مكتب الحوكمة والامتثال المؤسسي	منسوبي الجامعة		سارية	•
٣	CS-GRC-POL-1-V4.0	السياسة العامة للأمن السيبراني (عام- داخلي)	تعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات الجامعة الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.	٠٩-١١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الجامعة.	٠٣-٠٣-٢٠٢٥	سارية	• إدارة السياسات والإجراءات • إدارة الامتثال (Compliance) • الحوكمة

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٤	CS-SOC-POL-2-V4.0	سياسة اختبار الاختراق (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير في تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجامعة وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجامعة	٠٩-١١-٢٠٢١	إدارة الأمن السيبراني	تغطي جميع الأنظمة الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت (ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني والدخول عن بعد في الجامعة ،وتنطبق هذه السياسة على جميع العاملين الموظفين والمتعاقدين)	٠٤-٠٩-٢٠٢٤	سارية	• اختبارات الاختراق • أدوات فحص الثغرات • تقييم الأمان الدوري
٥	CS-GRC-POL-3-V3.0	سياسة إدارة الأصول المعلوماتية والتقنية (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة الأصول الخاصة بالجامعة لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية	٢٠-٠٢-٢٠٢٢	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول التقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في جامعة الأمير سطام بن عبدالعزيز.	٠١-٠٩-٢٠٢٤	سارية	• إدارة الأصول التقنية وحصرها • تصنيف الأصول التقنية • إدارة دوره حياه الاصول التقنية
٦	CS-SOC-POL-4-V4.0	سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير؛ لتقليل مخاطر الأمن السيبراني، وحماية الأصول المعلوماتية للجامعة من التهديدات (Threats) الداخلية والخارجية، عن طريق استخدام نظام إدارة سجلات الأحداث، ومراقبة الأمن السيبراني.	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع أنظمة إدارة سجلات الأحداث، ومراقبة الأمن السيبراني الخاصة بجامعه الأمير سطام بن عبدالعزيز ، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الجامعة	٢٤-٠٩-٢٠٢٤	سارية	• إدارة سجلات الاحداث • مراقبة الشبكات • تحليل التهديدات

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٧	CS-SOC-POL-5-V3.1	سياسة إدارة الثغرات (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية في جامعة الأمير سطام بن عبدالعزيز، وتنطبق هذه السياسة على جميع العاملين في الجامعة.	٠٩-٠٩-٢٠٢٤	سارية	• فحص الثغرات واكتشافها وتقييمها • إدارة التصحيحات ومعالجه الثغرات • تقارير الثغرات
٨	CS-GRC-POL-6-V4.0	سياسة إدارة حزم التحديثات والإصلاحات (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بجامعة الأمير سطام بن عبدالعزيز	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تطبق هذه السياسة على جميع الأصول التقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز بما فيها جميع المكونات التقنية للأنظمة التقنية السحابية (CTS) والأنظمة الحساسة والأنظمة التشغيلية وأنظمة العمل عن بعد والأصول التقنية الخاصة بحسابات التواصل الاجتماعي، وعلى إدارة الأمن السيبراني والإدارة العامة لتقنية المعلومات في الجامعة .	٠١-٠٩-٢٠٢٤	سارية	• Patch Management • تحديث الأنظمة وجدولة التحديثات • إدارة الإصدارات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات
٩	CS-SOC-POL-7-V5.0	سياسة إدارة حوادث وتهديدات الأمن السيبراني (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بالجامعة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.	٠٩-١١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق هذه السياسة على جميع العاملين (الموظفين والمتعاقدين) في الجامعة.	١٨-٠٦-٢٠٢٥	سارية	• تحليل التهديدات السيبراني • إدارة الحوادث السيبرانية والاستجابة لها

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
١٠	CS-GRC-POL-8-V4.0	سياسة إدارة كلمة المرور (مقيّد)	تقدم متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بكلمة المرور لحماية الجامعة من مخاطر الأمن السيبراني والتهديدات الداخلية والخارجية.	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	الهدف من هذه الوثيقة هو بيان السياسة الخاصة ببناء كلمة المرور للأنظمة والتطبيقات بالجامعة. مستخدمي هذه الوثيقة هم الموظفين وأعضاء هيئة التدريس ومن في حكمهم من المختصين.	٠٦-٠٢-٢٠٢٥	سارية	• إدارة كلمات المرور وانشائها وتخزينها • إدارة الحسابات والصلاحيات
١١	CS-GRC-POL-9-V4.0	سياسة إدارة مخاطر الأمن السيبراني (مقيّد)	تهدف إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في الجامعة وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية، والتقنية وتوافرها وسلامتها.	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية وأنظمة وأجهزة التحكم الصناعي الخاصة بجامعة الأمير سطام بن عبدالعزيز وإجراءات عمل الجامعة ، وتنطبق على جميع العاملين في الجامعة.	٢٤-٠٩-٢٠٢٤	سارية	• تقييم المخاطر • سجل المخاطر • تحليل الأثر • خطط معالجة المخاطر
١٢	CS-GRC-POL-10-V5.0	سياسة إدارة هويات الدخول والصلاحيات (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بالجامعة لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية	٠١-١٠-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين في الجامعة	٢٠-٠٦-٢٠٢٥	سارية	• إدارة الهوية والوصول • وإدارة الحسابات ذات الصلاحيات المميزة • وتطبيق الدخول الموحد • والتحكم في صلاحيات الوصول
١٣	CS-GRC-POL-11-V2.1	سياسة استخدام حسابات التواصل	الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل	٠٢-٠١-٢٠٢٢	إدارة الأمن السيبراني	تنطبق على الحسابات الخاصة بالجهات التابعة لجامعة الأمير سطام بن	٠٧-٠٦-٢٠٢٤	سارية	• إدارة حسابات التواصل الاجتماعي

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
		الاجتماعي (مقيّد)	الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بحسابات التواصل الاجتماعي في جامعة الأمير سطام بن عبدالعزيز تطبق بفعالية.			عبدالعزيز، وعلى حسابات منسوبي الجامعة ممن يمثل الجامعة رسميا.			• حماية الحسابات • مراقبة المحتوى
١٤	CS-GRC-POL-12-V4.1	سياسة الاستخدام المقبول للأصول التقنية (عام - داخلي)	تحديد متطلبات الأمن السيبراني؛ لتقليل مخاطر الأمن السيبراني، المتعلقة باستخدام أنظمة الجامعة وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.	١٠-٠١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة	٠٤-٠٧-٢٠٢٤	سارية	• تنظيم وإدارة ومراقبة استخدام الأصول التقنية • مراقبة سلوك المستخدمين • تعزيز الوعي الأمني لدى المستخدمين.
١٥	CS-GRC-POL-13-V5.0	سياسة الإعدادات والتحصين الآمن (مقيّد)	تحديد متطلبات الأمن السيبراني المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الأمير سطام بن عبدالعزيز للحد من المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في الجامعة للمحافظة على سرية المعلومات، وسلامتها، وتوافرها.	١٠-٠١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين في الجامعة	٢٦-٠٩-٢٠٢٤	سارية	• التحصين الأمني • وإدارة إعدادات الأنظمة والتطبيقات • وتطبيق معايير مركز أمن الإنترنت (CIS) للتحصين • ومراجعة الإعدادات بشكل

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
									دوري
١٦	CS-GRC-POL-14-V4.0	سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني (مقيّد)	تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن برنامج الأمن السيبراني لدى جامعة الأمير سطام بن عبدالعزيز يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.	٠١-١٠-٢٠٢١	إدارة الأمن السيبراني	تغطي جميع الأنظمة؛ والإجراءات الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين في الجامعة	١١-٠٥-٢٠٢٤	سارية	• متابعه الالتزام • التدقيق • اعداد التقارير والوثائق التنظيمية
١٧	CS-GRC-POL-15-V4.0	سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية (مقيّد)	تحديد متطلبات الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية في جامعة الأمير سطام بن عبدالعزيز من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة وفقا للسياسات والإجراءات التنظيمية الخاصة بالجامعة.	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية لجامعة الأمير سطام بن عبد العزيز، وتنطبق على جميع العاملين في الجامعة	١٧-٠٦-٢٠٢٥	سارية	• إدارة الموردين و إدارة العقود واتفاقيات مستوى الخدمة • تقييم مخاطر الأطراف الخارجية ومراقبة الامتثال بمتطلبات الأمن السيبراني وإجراء التقييم الأمني قبل التعاقد • إدارة وصول الأطراف الخارجية، والخدمات المدارة • ضمان حماية الوصول إلى

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
									أصول الجامعة التقنية.
١٨	CS-GRC-POL-16-V3.0	سياسة الأمن السيبراني المتعلق بالأمن المادي (مقيّد)	تحدد السياسة متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالأمن المادي في الجامعة تطبق بفعالية.	٢٢-٠٢-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأنظمة والأصول المعلوماتية والمعدات والأجهزة الخاصة بجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة	٢٤-٠٨-٢٠٢٤	سارية	• التحكم في الدخول • إدارة كاميرات المراقبة • أمن المرافق • مراكز البيانات

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
١٩	CS-GRC-POL-17-V4.0	سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (مقيّد)	توفر السياسة متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية الأصول المعلوماتية والتقنية الخاصة بالجامعة على خدمات الحوسبة السحابية والاستضافة Cloud Computing (Services and Hosting). وذلك، لضمان معالجة المخاطر السيبرانية أو تقليلها من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق هذه السياسة على جميع العاملين (الموظفين والمتعاقدين) في الجامعة . علمًا بأن قابلية تطبيق المتطلبات يعتمد على نوع خدمات الحوسبة السحابية المقدمة في الجامعة.	٠٤-٠٩-٢٠٢٤	سارية	• أمن الحوسبة السحابية • إدارة الهوية والوصول السحابي • حماية البيانات • التشفير • مراقبة التهديدات • إدارة الامتثال بمتطلبات الامن السيبراني • خدمات الاستضافة
٢٠	CS-GRC-POL-18-V4.0	سياسة الأمن السيبراني ضمن استمرارية الأعمال (مقيّد)	تحدد السياسة متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير ضمن إدارة استمرارية الأعمال لضمان استمرارية أعمال الجامعة وحمايتها من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على هدف التوافر وهو من الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة إدارة استمرارية الأعمال الخاصة بالأمن السيبراني في جامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة	٠٤-٠٩-٢٠٢٤	سارية	• إدارة استمرارية الأعمال • التعافي من الكوارث • خطط الطوارئ
٢١	CS-GRC-POL-19-V3.1	سياسة الأمن السيبراني للبيانات (مقيّد)	السياسة تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البيانات والمعلومات الخاصة بجامعة الأمير سطام بن عبد العزيز لتقليل مخاطر الأمن السيبراني وحمايتها من	٠٩-١١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع البيانات والمعلومات الخاصة بجامعة الأمير سطام بن عبد العزيز التي تتطلب إجراءات ومسؤوليات لحمايتها أثناء التخزين والنقل	٠١-٠٦-٢٠٢٥	سارية	• تصنيف البيانات • DLPحماية البيانات من الفقد • التشفير

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
			التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.			والوصول بما يتوافق مع المبادئ الأساسية لحماية البيانات، وتنطبق على جميع العاملين في الجامعة			• إدارة الوصول للبيانات
٢٢	CS-GRC-POL-20-V4.0	سياسة الأمن السيبراني للموارد البشرية (مقيّد)	تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في جامعة الأمير سطام بن عبد العزيز تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأنظمة الخاصة بجامعة الأمير سطام بن عبد العزيز وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الجامعة	٠٤-٠٢-٢٠٢٤	سارية	• إدارة ومتابعه الالتزام بالمتطلبات السيبرانية في دوره حياه الموظفين • التوعية بالأمن السيبراني
٢٣	CS-GRC-POL-21-V4.0	سياسة التشفير (مقيّد)	تقوم السياسة بتوفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة بجامعة الأمير سطام بن عبدالعزيز وللتقليل من المخاطر السيبرانية والتهديدات الداخلية والخارجية	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية الإلكترونية الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين في الجامعة ، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية	٠١-٠٩-٢٠٢٤	سارية	• تشفير البيانات، • إدارة مفاتيح التشفير PKI • حماية الاتصالات
٢٤	CS-GRC-POL-22-V4.0	سياسة الحماية من البرمجيات الضارة	السياسة توفر متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بجامعة	٠٩-٠٩-٢٠٢٤	سارية	• مكافحة البرمجيات الضارة، • EDR/XDR

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
		(مقيّد)	المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بجامعة الأمير سطام بن عبدالعزيز من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية			الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الجامعة			• تحديثات الحماية • فحص الأجهزة • حماية البريد الإلكتروني • حماية تصفح الانترنت • الاستجابة للحوادث
٢٥	CS-GRC-POL-23-V3.1	سياسة العمل عن بعد (مقيّد)	تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني للعمل عن بعد والتزام جامعة الأمير سطام بن عبدالعزيز بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية	٠٤-٠٣-٢٠٢٢	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة	٠٤-٠٩-٢٠٢٤	سارية	• الوصول عن بعد وإعداد VPN • إدارة الهوية والمصادقة متعددة العوامل • حماية الأجهزة إدارة الأجهزة المحمولة • حماية البيانات والتوعية الأمنية
٢٦	CS-GRC-POL-24-V4.0	سياسة النسخ الاحتياطية (مقيّد)	الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بالنسخ الاحتياطية لجميع المعلومات والأصول التقنية في الجامعة لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية	٠١-١٠-٢٠٢١	إدارة الأمن السيبراني	تطبق على الأصول المعلوماتية والتقنية (مثل: الأنظمة والبيانات والمعلومات) الخاصة بالجامعة ، وعلى جميع العاملين (الموظفين والمتعاقدين) في ال جامعة	٠١-٠٩-٢٠٢٤	سارية	• إدارة النسخ الاحتياطي وجدولته • تخزين النسخ الاحتياطية وحمايتها • استعادة النسخ الاحتياطية

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
			والخارجية						
٢٧	CS-GRC-POL-25-V4.0	سياسة أمن البريد الإلكتروني (مقيّد)	تحدد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البريد الإلكتروني لجامعة الأمير سطام بن عبدالعزيز من مخاطر الأمن السيبراني والتهديدات الداخلية والخارجية	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة	٠١-٠٩-٢٠٢٤	سارية	• حماية البريد الالكتروني • مكافحة التصيد • فلترة البريد • مراقبة الروابط والمرفقات
٢٨	CS-GRC-POL-26-V3.1	سياسة أمن الخوادم (مقيّد)	توفر متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers)الخاصة بجامعة الأمير سطام بن عبدالعزيز لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول التقنية والمعلوماتية (شاملة الخوادم) الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الجامعة .	٠٣-١٠-٢٠٢٣	سارية	• أمن الخوادم وإدارة الوصول • التحصين وإدارة التحديثات، • مراقبة السجلات والحماية من البرمجيات الضارة • النسخ الاحتياطية للخوادم • الاستجابة للحوادث
٢٩	CS-GRC-POL-27-V3.1	سياسة أمن الشبكات (مقيّد)	متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بجامعة الأمير سطام بن عبدالعزيز لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية .	١٤-٠٩-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الشبكات التقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة.	٠٣-١٠-٢٠٢٣	سارية	• حماية الشبكات ومراقبتها باستخدام جدران الحماية. • وأنظمة كشف ومنع التسلل • تطبيق مبدأ تقسيم الشبكات لتعزيز العزل الأمني
٣٠	CS-GRC-POL-28-V4.0	سياسة أمن أجهزة المستخدمين والأجهزة المحمولة	تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر الناتجة عن استخدام أجهزة المستخدمين	٠٥-٠٤-٢٠٢٢	إدارة الأمن السيبراني	تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين (الموظفين	١٥-٠٦-٢٠٢٥	سارية	• وإدارة الأجهزة المحمولة وحمايتها • وتطبيق آليات الكشف

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
		والأجهزة الشخصية (مقيّد)	(Workstations)، والأجهزة المحمولة (Devices Mobile)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") داخل الجامعة وحمايتها من التهديدات الداخلية والخارجية.			والمتعاقدين) داخل جامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة			والاستجابة للتهديدات، • وإدارة استخدام الأجهزة الشخصية.(BYOD)
٣١	CS-GRC-POL-29-V3.1	سياسة أمن قواعد البيانات (مقيّد)	توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية قواعد البيانات (Database) الخاصة بالجامعة لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية	١٠-٠١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع أنظمة قواعد البيانات الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في الجامعة	١٠-٠٣-٢٠٢٣	سارية	• حماية قواعد البيانات • وتشفير البيانات • ومراقبة الوصول • وإدارة أنشطة قواعد البيانات.
٣٢	CS-GRC-POL-30-V3.1	سياسة حماية تطبيقات الويب (مقيّد)	الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بالجامعة، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية	١٠-٠١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع تطبيقات الويب الخارجية الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق هذه السياسة على جميع العاملين في الجامعة	١٠-٠٣-٢٠٢٣	سارية	• حماية تطبيقات الويب، • تطبيق ممارسات البرمجة الآمنة • اختبار التطبيقات • فحص الثغرات الأمنية
٣٣	CS-GRC-POL-31-V1.0	سياسة دورة حياة تطوير البرمجيات الآمنة (مقيّد)	تحديد متطلبات الأمن السيبراني المتعلقة بدورة حياة تطوير البرمجيات الآمنة (SSDLC) لدى الجامعة. حيث تهدف السياسة إلى وضع البنود المناسبة التي تحكم عملية تطوير الأنظمة والبرمجيات لدى	١٠-٠٤-٢٠٢٣	إدارة الأمن السيبراني	تُطبق هذه السياسة على جميع الأنظمة والتطبيقات لدى جامعة الامير سطام بن عبدالعزيز سواءً تم تصميمها وتطويرها داخليًا أو بالاستعانة بأطراف خارجية، وتسري على جميع العاملين (الموظفين	-	سارية	• تطبيق ممارسات تطوير البرمجيات الآمنة • دمج الأمن في دورة التطوير • فحص الثغرات البرمجية • مراجعة الشيفرة البرمجية.

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
			الجامعة للحد من احتمالية وقوع هجمات الأمن السيبراني بسبب عدم ملائمة التصميمات أو الوظائف.			والمتعاقدين) في الجامعة			
٣٤	CS-GRC-POL-32-V1.1	سياسة حماية الأنظمة وأجهزة معالجة المعلومات (مقيّد)	توفر متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية الأنظمة وأجهزة معالجة المعلومات على الأصول المعلوماتية والتقنية الخاصة بالجامعة لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية	٠٤-٠١-٢٠٢٣	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز، وتنطبق على جميع العاملين في الجامعة	-	سارية	• حماية الأنظمة وأجهزة المعالجة وبياناتها • مراقبة الأداء والتحكم في صلاحيات الوصول • تطبيق آليات الكشف والاستجابة للتهديدات
٣٥	CS-GRC-POL-33-V2.0	سياسة أمن وسائط التخزين (مقيّد)	تحدد متطلبات الأمن السيبراني المتعلقة بوسائط التخزين المستخدمة في جامعة الامير سطام بن عبدالعزيز وتحديد عملية التخلص الآمن منها، وذلك لتقليل المخاطر السيبراني	٠٤-١٠-٢٠٢٣	إدارة الأمن السيبراني	تُطبق هذه السياسة على جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الامير سطام بن عبدالعزيز وعلى جميع العاملين (الموظفين والمتعاقدين) في الجامعة	٢٤-٠٩-٢٠٢٤	سارية	• تشفير وسائط التخزين • إدارة استخدامها والتخلص الآمن منها.
٣٦	CS-GRC-POL-34-V2.0	سياسة مركز البيانات (مقيّد)	وتهدف هذه السياسة إلى توفير متطلبات الامن السيبراني لحماية مراكز البيانات، بما يتماشى مع أفضل الممارسات والمعايير العالمية، ومتطلبات الهيئة الوطنية للأمن السيبراني.	٠٤-٠١-٢٠٢٣	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة	١٣-٠٥-٢٠٢٤	سارية	• إدارة وحماية مراكز البيانات • تطبيق ضوابط الأمن المادي وإدارة الطاقة والتبريد • مراقبة بيئة التشغيل.

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٣٧	CS-GRC-POL-35-V3.0	سياسة المخالفات والعقوبات (عام-داخلي)	تهدف السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بجامعة الأمير سطام بن عبدالعزيز، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك تهدف إلى تعزيز الوعي بأهمية الأمن السيبراني وضمان الامتثال للقوانين والتشريعات المتعلقة بالأمان السيبراني في المملكة العربية السعودية. وتهدف أيضًا إلى وضع إطار لتحديد الانتهاكات الأمنية وتحديد العقوبات المناسبة لها.	٠٤-٠٩-٢٠٢٣	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع المنتسبين للجامعة.	٢٤-٠٤-٢٠٢٥	سارية	• إدارة المخالفات الأمنية • متابعة الامتثال • تطبيق الإجراءات التأديبية.
٣٨	CS-GRC-POL-36-V1.0	سياسة المكتب الآمن والنظيف (عام -داخلي)	الغرض من هذه السياسة هو وضع متطلبات وإرشادات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتطبيق سياسة المكتب الآمن والنظيف في جامعة الأمير سطام بن عبدالعزيز، بما يسهم في تقليل المخاطر السيبرانية وحماية معلومات الجامعة من التهديدات الداخلية والخارجية	٠٣-٠٩-٢٠٢٣	إدارة الأمن السيبراني	تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع المنتسبين لجامعة الأمير سطام بن عبدالعزيز.	-	سارية	• تعزيز الوعي الأمني وتطبيق سياسة المكتب النظيف • حماية المستندات، وإدارة عرض الشاشات.

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٣٩	CS-GRC-POL-37-V3.0	سياسة مراجعة وتدقيق الأمن السيبراني (مقيّد)	تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لمراجعة وتدقيق ضوابط الأمن السيبراني لدى الجامعة والتأكد من تطبيقها وأنها تعمل وفقاً للسياسات والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على الجامعة	١٠-٠١-٢٠٢١	إدارة الأمن السيبراني	تغطي هذه السياسة جميع ضوابط الأمن السيبراني في جامعة الأمير سطام بن عبدالعزيز وتنطبق على جميع العاملين في الجامعة.	٠٤-٠٣-٢٠٢٣	سارية	• تنفيذ أعمال التدقيق الداخلي • ومراجعة الضوابط الأمنية، وإعداد تقارير الامتثال • دعم التحسين المستمر.
٤٠	CS-GRC-POL-38-V5.0	أدوار ومسؤوليات الأمن السيبراني (مقيّد)	الوثيقة تحدد أدوار ومسؤوليات الأمن السيبراني في الجامعة لتحقيق الغرض الأساسي منها وهو التأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجامعة على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني في الجامعة والجهات التابعة لها	٠٩-١١-٢٠٢١	إدارة الأمن السيبراني	تطبق هذه الوثيقة على جميع العاملين (الموظفين والمتعاقدين) في جامعة الأمير سطام بن عبدالعزيز.	٠٥-١١-٢٠٢٤	سارية	• تحديد الأدوار والمسؤوليات • توزيع المهام والصلاحيات • حوكمة الأمن السيبراني • متابعة الالتزام • المساءلة والمحاسبة
٤١		سياسة مراجعة اللوائح والقواعد الأساسية بالجامعة	ضوابط عامة لمراجعة التنظيمات بأنواعها	27/04/25	مكتب الرئيس	جميع القرارات واللوائح الصادرة من الجامعة		سارية	•
٤٢						جميع أنشطة البحث والتطوير الممولة مصادر الجامعة الذاتية، أو غير الممولة، والتي مت إنتاجها من طرف أحد منسوبي		سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
						الجامعة، أو الممولة عن طريق ما يتم تخصيصه من ميزانية الدولة للجامعة، أو الممولة عن طريق جهات أخرى، أو ممولة بواسطة شركاء الجامعة، ويستثنى من ذلك المشاريع المشتركة التي تكون وفق اتفاقيات تعاقدية ممولة من قبل القطاع الخاص، ومحددة مخرجات لتكون لصالح القطاع اخلاص			
٤٣		سياسة المسؤولية المجتمعية	معايير وحدود المسؤولية المجتمعية	2024	إدارة المسؤولية المجتمعية	مجتمع مدينة الخرج		سارية	•
٤٤		سياسة البيانات المفتوحة	تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع المعنيين في الجامعة بأعمال البيانات المفتوحة	10/07/21	الإدارة العامة لتقنية المعلومات	جميع البيانات العامة في الجامعة	17/7/2025	سارية	•
٤٥		سياسة الخصوصية		21/11/2024	الإدارة العامة لتقنية المعلومات	جميع فروع الجامعة التي تقوم كليا أو جزئياً بمعالجة البيانات والمستفيدين من خدمات الجامعة، والجهات الخارجية التي تقوم بمعالجة البيانات.		سارية	•
٤٦		سياسة تصنيف البيانات	تهدف هذه السياسة إلى وضع المبادئ الأساسية وضوابط تصنيف البيانات في	10/07/21	الإدارة العامة لتقنية	جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها	18/9/2025	سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
			الجامعة مهما كان مصدرها أو شكلها أو طبيعتها. وكذلك وضع إطار موحد لتصنيف البيانات إلى أربعة مستويات بناءً على نتائج تقييم الأثر المترتب على الإفصاح غير المصرّح به نظاماً عن البيانات أو عن محتواها، بحيث يحدد هذا الإطار آلية الاطلاع على البيانات والتعامل معها وفقا لمستوى تصنيفها.		المعلومات	أو شكلها أو طبيعتها			
٤٧		سياسة حرية المعلومات	تهدف هذه السياسة الى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع المعنيين في الجامعة بأعمال حرية المعلومات . والتي تنظم حق الاطلاع أو الحصول على المعلومات العامة التي تنتجها الجامعة وذلك تعزيز المبدأ الشفافية	10/07/21	الإدارة العامة لتقنية المعلومات	جميع طلبات الأفراد للاطلاع أو الحصول على المعلومات العامة التي تنتجها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها	18/9/2025	سارية	•
٤٨		سياسة حماية البيانات الشخصية	معلومات عامة عن البينات التي تتعامل مع مواقع الجامعة وخدماتها الإلكترونية	10/07/21	الإدارة العامة لتقنية المعلومات	جميع فروع الجامعة	17/7/2025	سارية	•
٤٩		سياسة تكامل البيانات ومشاركتها	تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع أصحاب المصلحة المعنيين في الجامعة بأعمال تكامل البيانات ومشاركتها.	17/7/2025	الإدارة العامة لتقنية المعلومات	جميع فروع الجامعة التي تقوم كليا أو جزئياً بمعالجة البيانات في الجامعة	18/9/2025	سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٥٠		سياسة البوابة : القواعد والإرشادات التي وضعتها الإدارة لتنظيم العلاقة بينها وبين الزوار أو المستخدمين لبوابة الجامعة.	إرشادات عامة	21/11/2024	الإدارة العامة لتقنية المعلومات	عام		سارية	•
٥١		سياسة استمرارية الأعمال	إن الغرض من هذه السياسة هو تحديد القواعد الأساسية لإدارة استمرارية الأعمال . ويتم تطبيق هذه السياسة على كامل نظام إدارة استمرارية الأعمال	23/9/2024	الإدارة العامة لتقنية المعلومات	جميع الإدارات والوحدات التابعة للجامعة التي تقدم خدمات تقنية أو أكاديمية أو إدارية تعتمد على أنظمة المعلومات	23/9/2024	سارية	•
٥٢		سياسة استخدام خدمة الدخول عن بعد VPN	معايير منح صلاحيات الخدمة وضوابطها	15/7/2025	الإدارة العامة لتقنية المعلومات	جميع موظفي الجامعة، وأعضاء هيئة التدريس، والمتعاونين، والموردين الذين يُمنحون صلاحية الاتصال عن بعد بشبكة الجامعة عبر خدمة الVPN، باستخدام الأجهزة المعتمدة فقط	15/7/2025	سارية	•
٥٣		سياسة الحوسبة السحابية	تنظيم وتوجيه عمليات تبني، ونقل، وتشغيل، وإدارة خدمات الحوسبة السحابية داخل الجامعة بما يضمن الاستفادة القصوى من مزاياها وتحقيق الكفاءة والمرونة والابتكار	23/7/2025	الإدارة العامة لتقنية المعلومات	جميع الإدارات والوحدات بالجامعة التي تستخدم أو تخطط لاستخدام خدمات الحوسبة السحابية	45815	سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٥٤		سياسة ضوابط إدارة النسخ الاحتياطي وحماية البيانات	تنظيم عملية النسخ الاحتياطي للبيانات المهمة	23/7/2025	الإدارة العامة لتقنية المعلومات	جميع الأنظمة والخوادم وقواعد البيانات التابعة للجامعة، سواء في مراكز البيانات أو في البيئات السحابية، وتشمل النسخ الاحتياطي للبيانات الأكاديمية، والمالية، والإدارية، وبيانات المستخدمين.	23/7/2025	سارية	•
٥٥		سياسة استخدام البريد الإلكترون	تحدد هذه الوثيقة السياسة والإجراءات الخاصة للاستخدام المقبول للبريد الالكتروني الجامعي والحقوق والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدمها	27/6/2025	الإدارة العامة لتقنية المعلومات	جميع مستخدمي البريد الإلكتروني الرسمي للجامعة (الموظفين، وأعضاء هيئة التدريس، والطلاب، والمتعاونين)، سواء تم الوصول للبريد من داخل أو خارج شبكة الجامعة	08/07/25	سارية	•
٥٦		سياسة استخدام أجهزة الهاتف الشبكي	تحدد هذه الوثيقة السياسة والإجراءات الخاصة للاستخدام المقبول لأجهزة الهواتف الشبكية والحقوق والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدمها	27/6/2025	الإدارة العامة لتقنية المعلومات	جميع الإدارات التي تستخدم أنظمة الهاتف الشبكي	08/07/25	سارية	•
٥٧		سياسة استخدام أجهزة الحاسب الآلي	تحدد هذه الوثيقة السياسة والإجراءات الخاصة للاستخدام المقبول لأجهزة الحاسب الآلي والحقوق والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدمها	27/6/2025	الإدارة العامة لتقنية المعلومات	جميع أجهزة الحاسب الآلي المكتبية والمحمولة المملوكة للجامعة أو المستخدمة ضمن بيئة العمل الجامعية، بما يشمل العاملين، وأعضاء هيئة التدريس، والطلاب في المعامل والمكاتب	08/07/25	سارية	•
٥٨		سياسة استخدام شبكة الأنترنت	تحدد هذه الوثيقة السياسة والإجراءات الخاصة للاستخدام المقبول لشبكة الأنترنت والحقوق	27/6/2025	الإدارة العامة لتقنية المعلومات	جميع مستخدمي شبكة الإنترنت الخاصة بالجامعة، سواء من خلال الاتصال السلكي أو اللاسلكي (Wi-Fi)، وتشمل	08/07/25	سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
			والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدمها			الطلاب، وأعضاء هيئة التدريس، والإداريين، والزوار.			
٥٩		سياسة استخدام الأجهزة التعليمية	تحدد هذه الوثيقة السياسة والإجراءات الخاصة للاستخدام المقبول لأجهزة مصادر التعلم وتقنيات التعليم والحقوق والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدمها	27/6/2025	الإدارة العامة لتقنية المعلومات	كافة مستخدمي الأجهزة التعليمية بالجامعة	08/07/25	سارية	•
٦٠		سياسة طلب الخوادم	تحدد هذه الوثيقة السياسة والإجراءات الخاصة لطلب خادم أو استضافة خادم والحقوق والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدمها	27/6/2025	الإدارة العامة لتقنية المعلومات	جميع الإدارات والوحدات الأكاديمية التي تطلب توريد أو تشغيل خوادم (Servers) جديدة، سواء داخل مراكز البيانات أو في البيئات السحابية الخاصة بالجامعة.	08/07/25	سارية	•
٦١		سياسة إدارة الوصول لمراكز البيانات والإجراءات التشغيلية	تحديد معايير وضوابط الدخول لمراكز البيانات	27/6/2025	الإدارة العامة لتقنية المعلومات	جميع مراكز البيانات التابعة للجامعة وجميع الموظفين أو المتعاقدين المصرح لهم بالوصول المادي أو المنطقي إليها	08/07/25	سارية	•
٦٢		سياسة حوكمة البيانات	تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمواصفات المسؤوليات التي يجب الامتثال لها من قبل جميع الموظفين، المنتسبين، المشغلين وجميع الجهات والأفراد التي تعمل مع الجامعة أو تتعامل معها	30/8/2025	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٦٣		سياسة جودة البيانات	تهدف هذه السياسة الى تحديد المبادئ الرئيسية والضوابط الأساسية لضمان صحة ودقة البيانات في الجامعة وتحديد المسؤوليات المتعلقة بمراقبة جودة البيانات فيها وقياس حالة البيانات من حيث الدقة، والاكتمال، والاتساق، والموثوقية.	30/8/2025	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•
٦٤		سياسة تخزين البيانات	تهدف هذه السياسة إلى تحديد المبادئ لرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع المعنيين في لجامعة ف ي جمي ع المراحل الت ي تم ر بها البيانات في الجامعة، والتي تبدأ من جمعها، ثم تخزينها بطريقة آمنة لاستبقائها خلال لفترة المحدد ة لها، مرور ا بالنسخ الاحتياطي لها، وبعد ذلك يتم التخلص منها بطرق الإتلاف المعتمدة داخل الجامعة، وذلك وفقًا للفترة الزمنية التي تقتضيها متطلبا ت الأعمال ل أو المتطلبات التشريعية	30/8/2025	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•
٦٥		سياسة تحقيق القيمة من البيانات	تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع المعنيين في الجامعة بأعمال تحقيق الإيرادات من البيانات	08/04/25	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
٦٦		سياسة النمذجة وحوكمة البيانات	تهدف هذه السياسة الى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع المعنيين في الجامعة بتمثيل البيانات وتبسيطها من خلال نمذجة تلك البيانات وهيكلتها عن طريق تحديد مجموعة من الإجراءات والأنظمة والهياكل التنظيمية المطلوبة لحفظ البيانات والوصول إليها ونقلها وتنظيمها.	09/04/25	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•
٦٧		سياسة البيانات الوصفية ودليل البيانات	تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع منسوبي الجامعة المعنيين بأعمال تعريف وإدارة البيانات الوصفية ودليل البيانات	09/04/25	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•
٦٨		سياسة ادارة البيانات المرجعية	تهدف هذه السياسة إلى تحديد المبادئ الرئيسية والضوابط والمسؤوليات التي يجب الامتثال لها من قبل جميع المعنيين في الجامعة، سواء كانوا مسؤولين عن إدارة البيانات المرجعية والرئيسية أو مستخدمين لها	09/04/25	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•
٦٩		سياسة ذكاء الاعمال والتحليلات	تهدف هذ السياسة الى تحديد المبادئ الرئيسية لجمع وتحليل البيانات الداخلية والخارجية لاستخلاص	30/8/2025	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•

م	رقم السياسة	عنوان السياسة	وصف مختصر للسياسة	تاريخ الإصدار	مالك السياسة	نطاق التطبيق	تاريخ التعديل	حالة السياسة (سارية/ معطلة)	الخدمات المرتبطة
			المعرفة والقيمة منها، كما تحدد الضوابط المطلوبة التي تمكن عملية عر ض البيانات ولوحا ت المؤشرات لاستخدامها من قبل الأعمال والاستفادة منها.						
٧٠		سياسة ادارة المحتوى والوثائق	تهدف هذه السياسة الى تحديد المبادئ الرئيسية والضوابط لضمان الحفاظ على البيانات والمعلومات وتحقيق الاستخدام الأمثل والفعال لها في صيغتها غير المهيكلة، وتحويلها إلى بيانات بصيغ مهيكلة لتسهيل استخدامها والاستفادة منها .	30/8/2025	الإدارة العامة لتقنية المعلومات	كامل نطاق الجامعة		سارية	•
٧١		سياسة ضمان جودة التعليم والتعلم	تهدف هذه السياسة إلى ضمان جودة العملية التعليمية في جميع البرامج الأكاديمية من خلال معايير لمتابعة الأداء الأكاديمي	04/03/2026	عمادة التطوير والجودة	الكليات		سارية	•
٧٢		سياسة الاستثمار	تهدف هذه السياسة إلى تحديد منهجية الاستثمار في الجامعة وحدود وقيود الاستثمار.	23/5/2022	الإدارة العامة للاستثمار والأوقاف	أصول جامعة الأمير سطام بن عبدالعزيز المادية أو المالية			•
٧٣		سياسة المشتريات	تحديد الضوابط العامة للمشتريات	٢٠٢٢	إدارة المشتريات	جميع وحدات الجامعة		سارية	• المشاريع • الشراء المباشر • التعاقد • المنافسات