سياسة أمن البريد الإلكتروني

V2.1

تفاصيل الوثيقة

اسم الوثيقة	سياسة أمن البريد الإلكتروني
تصنيف الوثيقة	مقيد ج
رقم آخر إصدار	2.1
نوع الوثيقة	تحديث
مالك الوثيقة	إدارة الأمن السيبراني
مرجعية الوثيقة	ISO/IEC 27001:2013 NCA ECC-1:2024 ISO 22301:2019 Best practice

جدول التعديلات على الوثيقة

وصف التغيير	تم الإعداد بواسطة	رقم الإصدار	التاريخ
إعداد الوثيقة	إدارة الأمن السيبراني	1.0	02-سبتمبر-2021
1- تحديث مسمى "إدارة أمن المعلومات" داخل المستند الى "إدارة الأمن السيبراني" 2- ترقيم البنود 3- فصل سياسة "أمن البريد الالكتروني"	إدارة الأمن السيبراني	1.1	13-مارس-2022
إضافة بنود عامة	إدارة الأمن السيبراني	1.2	21-فبراير-2023
1- تحديث مسمى "عمادة تقنية المعلومات" داخل المستند الى "الإدارة العامة لتقنية المعلومات"	إدارة الأمن السيبراني	1,3	18-ديسمبر-2023
مراجعة الوثيقة لاعتمادها	إدارة الأمن السيبراني	2	9-يونيو-2024
إضافة بند "يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دوريا."	إدارة الأمن السيبراني	2.1	26-يناير-2025

جدول مراجعة الوثيقة

تمت المراجعة بواسطة	التاريخ	التوقيع	تاريخ المراجعة القادم
مدير إدارة الأمن السيبراني " م. خالد إبراهيم الفيفي"	2021/10/10		مارس 2022
نائب مدير إدارة الأمن السيبراني "سامر محمد أحمد الضويمر"	2022/5/26		مارس 2023
رئيسة قسم الحوكمة والمخاطر والإلتزام "خلود فرج العمراني"	2023/2/21		مارس2024
رئيسة قسم الحوكمة والمخاطر والإلتزام "خلود فرج العمراني"	2024/4/15		ابريل 2025

جدول اعتماد الوثيقة

تم الاعتماد بواسطة	التاريخ	التوقيع
رئيس جامعة تبوك	2021/10/11	
رئيس جامعة تبوك	2022/5/29	
اللجنة الإشرافية للأمن السيبراني	2023/2/28	

جدول المحتويات

1. المقدمة

تُمَثِّل هذه الوثيقة سياسة أمن البريد الإلكتروني الخاصة بجامعة تبوك والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من تِسعة أقسام رئيسية لِتَشمل هذه المُقَدِمَة يليها الغَرض، والنطاق، والأدوار والمسؤوليات، وبنود السياسة، والمرجعيات، والالتزام، ومعايير الاستثناءات، وأخيراً المصطلحات والتعريفات.

على جَمِيع المستخدمين القيام بالقراءة المُتأنِية والفهم الجيد والالتزام الكامل بسياسة أمن البريد الإلكتروني. وفى حالة عدم الاستيعاب أو عدم الفهم الكامل من قِبَل أي مستخدم لتلك الوثيقة أو لأي جزءٌ منها، فإنه يَجِب عليه التواصل في الحال مع إدارة الأمن السيبراني حتى يتسنى له فهم النِقَاط غير الواضحة بالنسبة له.

تُعَدُ إدارة الأمن السيبراني بالجامعة هي المالكة لِتلك الوثيقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على إدارة الأمن السيبراني مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، أو يجوز أيضاً تحديثها فور حُدوث أى تعديلات أو تغييرات تَتَعَلَّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تَغيير رقم إصدار الوثيقة حال القِيام بأى تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ اللجنة الإشرافية للأمن السيبراني بالجامعة.

2. الغرض

تهدُف هذه السياسة إلى التعامل الآمن مع البريد الالكتروني وذلك لتخفيف المخاطر، وكذلك العمل على حِماية سرية وسلامة وتوافر الأصول التقنية والمعلوماتية داخل الجامعة.

3. النطاق

تنطبق هذه الوثيقة على كافة الأصول المعلوماتية والتقنية والخدمات المقدمة، وكذلك كافة مستخدميها من الموظفين سواء كانوا يعملون بصفة دائمة أو مؤقتة، أو يعملون بدوام كامل أو دوام جزئي، أو متعاقدين كموظفي شركات الإسناد الخارجي. وكذلك مستخدمي وموظفي جميع الأطراف الخارجية كالمقاولين والموردين والشركات الاستشارية والجهات الحكومية وشركات الخدمات المُدارة والشركات والجهات الخاصة بالاستضافة والحوسبة السحابية وغيرها.

4. الأدوار والمسؤوليات

المسؤول	الإعداد والمراجعة والتحديث	الاعتماد	النشر	الالتزام والتطبيق
اللجنة الإشرافية للأمن السيبراني				
إدارة الأمن السيبراني				
الإدارة العامة لتقنية المعلومات				

5. بنود السياسة

5.1 السياسة العامة

5.1.1 عند الحصول على صلاحية (all) للبريد الإلكتروني الخاص بجامعة تبوك فإنه يجب على جميع منسوبي جامعة تبوك (موظفين، أعضاء هيئة التدريس، طلاب) الالتزام بالضوابط التالية:

- لا يحق لأي جهة داخل الجامعة أو منسوبي الجامعة الحصول على صلاحية الجميع (all) إلا بعد رفع طلب للإدارة العامة لتقنية المعلومات وإرفاق المبررات الكافية للحصول على الصلاحية مع شرط تخصيص الفئة المستهدفة (أعضاء هيئة التدريس)، (الموظفين) ، (الطلاب) وتحديد المدة الزمنية لاستخدام الصلاحية وعدد الرسائل التي سيتم استخدامها شهريا وأخذ موافقة إدارة الأمن السيبراني للحصول على الصلاحية.
- يجب على الجهات داخل الجامعة أو منسوبي الجامعة الذين تم منحهم الصلاحيات بالإلتزام بالمبررات المقدمة لإدارة الأمن السيبراني للحصول على الصلاحية.
- يجب تحديد مدة محددة لإستخدام خدمة الإرسال (all) والإلتزام بالمدة مع قابلية تمديد المدة بعد أخذ الموافقات اللازمة.
- يجب على الجهة داخل الجامعة أو منسوبي الجامعة الممنوحة لهم صلاحية الجميع (all) الإلتزام بعدد الرسائل المتفق عليها مسبقا.
- يجب على الجهة داخل الجامعة أو منسوبي الجامعة الممنوحة لهم صلاحية الجميع (all) مراعاة المحتوى والإلتزام بمضمون الجهة وعدم الخروج عنه.
- يجب على الإدارة العامة لتقنية المعلومات مراجعة قائمة الجهات ومنسوبي الجامعة الممنوحة لهم صلاحية الجميع (all) وتحديثها سنويا.
- يحق الإدارة العامة لتقنية المعلومات أو إدارة الأمن السيبراني إلغاء صلاحية الجميع(all) من منسوبي الجامعة أو الجهات داخل الجامعة حسب ما تقتضيه المصلحة أو ما تراه مناسبا بدون الحاجة إلى إشعار الجهة أو الشخص.
- يحق لإدارة الأمن السيبراني منح صلاحية الجميع (all) لإي جهة داخل الجامعة أو منسوبي الجامعة حسب ما تراه مناسبا أو تقتضيه الحاجة.
- يحق لإدارة الأمن السيبراني تجميد أي حساب بريد إلكتروني داخل نطاق جامعة تبوك سواء كان لموظف أو عضو هيئة تدريس أو طالب حسب ما تراه الإدارة مناسبا أو تقتضيه الحاجة.

5.1.2 عند استخدام البريد الإلكتروني في الأجهزة المتنقلة مثل الهواتف الذكية، فيجب على الجهة داخل جامعة تبوك أو منسوبي الجامعة تزويد الأجهزة المتنقلة بميزة قفل الأمان التلقائي وكلمة السر في حالة عدم استخدام الجهاز.

5.1.3 يحظر على الجهات داخل جامعة تبوك أو منسوبي الجامعة المشاركة في نشر رسائل البريد الإلكتروني لأسباب شخصية أو تجارية أو دينية أو سياسية.

5.1.4 يجوز للجهات داخل جامعة تبوك أو منسوبي الجامعة تبادل المعلومات عبر البريد الإلكتروني وفقاً لإجراءات تصنيف البيانات ومعالجة المعلومات.

5.1.5 يقصر استخدام البريد الإلكتروني لجامعة تبوك على المراسلات الرسمية المتعلقة بالعمل فقط.

5.1.6 لا يسمح باستخدام أي بريد إلكتروني شخصي في المراسلات الرسمية المتعلقة بالعمل.

5.1.7 عدم إرسال كلمات المرور عن طريق البريد الإلكتروني.

5.1.8 عدم فتح أي رابط من رسائل البريد الإلكتروني غير معروفة المصدر، وفي حالة معرفة المصدر لابد من التحقق من عنوان المرسل وصحة الرابط قبل فتح الرابط.

5.1.9 يجب على جميع المستخدمين التبليغ في حالة الاشتباه في أحد الرسائل أنها رسائل تصيد احتيالي إلى إدارة الأمن السيبراني بالجامعة عبر البريد الالكتروني: ut.soc@ut.edu.sa

5.1.10 اتباع سياسات الجامعة عند انشاء كلمة مرور.

5.2 حماية البريد الإلكتروني

5.2.1 يجب على الإدارة العامة لتقنية المعلومات التأكد من حماية خدمات البريد الإلكتروني من أي مخاطر سيبرانية وكذلك من هجمات الأمن السيبراني.

5.2.2 يجب حماية خدمات البريد الإلكتروني من أي وصول غير مُصرَّح به، أو أي إفشاء للمعلومات، أو رسائل التصيد الاحتيالي، أو رسائل البريد العشوائي أو البرامج الضارة غير المعروفة مسبقاً، باستخدام ضوابط الأمن السيبراني المناسبة مثل: خصائص مكافحة البريد العشوائي، وخصائص مكافحة التصيد، وإطار عمل سياسة المُرسل، وفحص رسائل البريد الإلكتروني ضد الفيروسات والملفات الضارة وهجمات (zero day attacks) والبرمجيات الضارة غير المعروفة مسبقاً، وما إلى ذلك.

5.2.3 يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.

5.2.4 يجب فحص جميع رسائل البريد الإلكتروني، سواء الداخلية أو الخارجية، ضد أي هجمات أو مخاطر تتعلق بالأمن السيبرانى، وليس فقط البريد الإلكتروني الخارجي، لتجنب انتشار مصدر هجوم داخلي في بيئة عمل الجامعة.

5.2.5 يجب التحكم في الوصول إلى البريد الإلكتروني الخارجي وتأمينه باستخدام التحقق من الهوية مُتعدِّد العناصر لحماية المعلومات من الكشف والوصول غير المُصرَّح به وما إلى ذلك.

5.2.6 يحظر على جميع الموظفين والمستخدمين إستخدام البريد الإلكتروني الخاص بالعمل في أي منتديات أو مواقع عامة لتقليل البريد العشوائي، أو رسائل التصيد الإحتيالي أو البرامج الضارة التي قد تأتي من هذه المواقع العامة غير الموثوق بها.

5.2.7 يُعتَبَر النسخ الاحتياطي لخادم البريد الإلكتروني والنسخ الاحتياطي لقاعدة البيانات أحد أهم الجوانب التي تساهم في تأمين وحماية خدمة البريد الإلكتروني.

5.2.8 يجب على الإدارة العامة لتقنية المعلومات بالجامعة استخدام خصائص وبرامج الحماية المتقدمة من التهديدات المستمرة (APT) لحماية خوادم البريد الإلكتروني من أي برمجيات ضارة غير معروفة مسبقاً، أو فيروسات، أو ملفات ضارة، وللتصدى ضد أي هجمات مُعقَّدة تستهدف البيانات السرية.

5.2.9 يُعتبَر وعي المستخدم، أحد الجوانب الرئيسية لحماية خدمة البريد الإلكتروني من أي رسائل تصيد أو بريد عشوائي وما إلى ذلك، ويؤدى الوعي إلى زيادة مستوى الأمان الذي يقلل بدوره أي تهديدات أو هجمات سيبرانية.

5.2.10 يُعَدُّ توثيق نطاق البريد الإلكتروني للأطراف المُرسلة من خلال بعض الادوات التقنية، مثل إطار سياسة المرسل، أحد أساليب الحماية لزيادة حماية البريد الإلكتروني وأمنه.

5.2.11 يجب توثيق مجال البريد الإلكتروني للجامعة عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email

Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).

5.2.12 يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.

5.2.13 يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.

5.2.14 يجب تطبيق التقنيات اللازمة لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.

5.2.15 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.

5.2.16 يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

5.2.17 يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دوريا.

6. المرجعيات

- ECC-1:2018, 2-4

7. الالتزام

- يجب أن تتوافق سياسة أمن البريد الإلكتروني مع الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (ECC:1-2018) ومع جميع متطلبات معيار الأيزو العالمي لأمن المعلومات (ISO/IEC 27001:2013) و (ISO 22301:2019) وكافة المتطلبات التشريعية و التنظيمية والتعاقدية.
- ينبغي الالتزام بسياسة أمن البريد الإلكتروني من قِبَل جميع المستخدمين والموظفين والأطراف المعنية ذات العلاقة، ويجب على جميع مدراء الإدارات والأقسام التَأَكُد من الالتزام المُستَمر بتطبيقها.
- يَنبغي مُراجعة الالتزام بتَطبيق السياسة دَورياً بواسطة إدارة الأمن السيبراني, كما يَجِب على الإدارة العليا اتخاذ كافة الإجراءات التصحيحية اللازمة حال حدوث أي انتهاك للسياسة. ويجب أنَّ تَتكافأ حِدّة الإجراءات التأديبية مع حجم الانتهاك أو جَسامة الحادِث المُرتَكَب، ويَتَحَدَّدْ ذلك عَقب الانتهاء من التحقيقات اللازمة والتي بِدورها قد تُسفِر عن التالي، على سبيل المثال لا الحصر:
  - فَقْدْ امتيازات الوصول إلى الأصول المعلوماتية والتقنية.
  - تطبيق بعض العقوبات يكون حَسبما تَراه الإدارة العليا مناسباً وفق الأنظمة والتعليمات والتشريعات من الهيئة الوطنية للأمن السيبراني والقوانين الرسمية الخاصة بالجرائم المعلوماتية.

8. معايير الاستثناءات

- تَهْدُف هذه الوثيقة إلى تَلبِية جميع مُتطلّبات الأمن السيبراني. وبُنَاءً عليه, يَجِب تَقديم طَلَبْ رَسمِي، عند الحاجة إلى الحُصول على استثناء. ويُقَدَّم الطَلب إلى إدارة الأمن السيبراني, مع ذِكْر حيثيات طلب الاستثناء بوضوح، وعَرْض الفوائد المَرجُوَّة من هذا الاستثناء، ليتم البَتّ فيه ومَنْح الموافقة النِهائية من قِبَلْ مدير إدارة الأمن

السيبراني أو اللجنة الإشرافية للأمن السيبراني ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

- تَصِل فترة الاستثناء لمُدَّة عام واحد كَحدّ أقصى, إلَّا أنَّه يُجوز إعادة تقييم طَلَب الاستثناء وتَجدِيد المُوافقة عليه بحد أقصى ثلاث أعوام متتالية إذا اقتضَى الأَمر، ولا يَجُوز مَدّ العَمَل بالاستثناء لفترات أُخرى بعد انتهاء الثَّلاث أعوام السالِف ذِكْرِهُم.

9. المصطلحات والتعريفات

المصطلح	التعريف
الأمن السيبراني	حسب ما نص عليه تنظيم الهيئة الوطنية للأمن السيبراني، الصادر بالأمر الملكي رقم (6801) وتاريخ (1439/2/11هـ) فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
NCA	الهيئة الوطنية للأمن السيبراني.
ISO	المنظمة الدولية للمعايير (منظمة الأيزو).
ECC	الضوابط الأساسية للأمن السيبراني.
الأصل	أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
السرية	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.
سلامة المعلومات	الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات والموثوقية.
التَوافُر	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
حادِثة	انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني
التَحَقّق	التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام
صلاحية المستخدم	خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى بعض الموارد وكذلك أمن الأصول المعلوماتية والتقنية للجهة بصفة عامة وضوابط الوصول بصفة خاصة.
ضابط	مقياس لتقييد و معالجة المخاطر.
المخاطر السيبرانية	المخاطر التي تَمِسّ عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية

	الوصول غير المُصَرَّح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نُظم المعلومات.
الحِماية من التهديدات المتقدمة المستمرة APT	الحِماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحِماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) لتحقيق هدفه.
رسائل التصيد الإلكتروني	محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الإئتمان، غالباً لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.
منسوبي الجامعة	يشمل مصطلح منسوبي الجامعة الموظفين وأعضاء هيئة التدريس و طلاب الجامعة.