KINGDOM OF SAUDI ARABIA
Ministry of Education
KING ABDULAZIZ UNIVERSITY
CyberSecurity Center

المملكة العربية السعودية
وزارة التعليم
جامعة الملك عبد العزيز
مركز الأمن السيبراني

مركز الأمن السيبراني
CyberSecurity Center

سياسة الاستخدام المقبول للأصول

Assets Acceptable Use Policy

CSC-Pol-02
الإصدار Version 4.0

التصنيف: عام
Classification: General

اعتماد الوثيقة

الدور Role	المسمى الوظيفي Job Title	الاسم Name	التاريخ Date	التوقيع Signature
المالك	مدير مركز الأمن السيبراني	د. ريان بن هشام موصلي Dr. Rayan Hisham Mosli	٢٠٢٥/٤/٢٧	
المصرّح	رئيس الجامعة	د. طريف بن يوسف الأعمى Dr. Tareef Yousuf Alaama	٢٠٢٥/٤/٢٢م	

نسخ الوثيقة

النسخة Version	التاريخ Date	عُدّل بواسطة Edited By	أسباب التعديل Reasons of Modification
1.0	١٤٤٣/٤/١٠ هـ 15/11/2021	خالد بن عطية الله الصبحي Khalid Attyah Alsubhi	
2.0	١٤٤٤/٤/٢٠ هـ 14/11/2022	دانيال بن محمد الغزاوي Daniyal Mohammed Alghazzawi	بناء على متطلبات هيئة الأمن السيبراني
3.0	١٤٤٥/٦/١٩ هـ 1/1/2024	دانيال بن محمد الغزاوي Daniyal Mohammed Alghazzawi	دمج النسخة العربية مع الإنجليزية وإضافة الوثائق الخاصة بخطط استمرارية الأعمال Merging the Arabic version with the English version and added the documents for the Business Continue Plan
4.0	١٤٤٦/٠٢/١٢ هـ 18/08/2024	مرام بنت خالد حمبيشي Maram Khalid Hambishi	بناء على متطلبات الهيئة According to the requirements of the Authority

جدول المراجعة

معدل المراجعة Review Period	التاريخ Date	تمت المراجعة بواسطة Revised By
مرة واحدة كل سنة	١٤٤٦/٤/٢٦ هـ 29/10/2024	د. ريان بن هشام موصلي Dr. Rayan Hisham Mosli

قائمة المحتويات

INDEX

الاهداف

Objectives

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة جامعة الملك عبد العزيز وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها،

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

The purpose of this policy is to provide and guarantee the necessities of cybersecurity in such a way as to reduce cybersecurity risks relating to the use of King AbdulAziz University systems and assets, to protect said systems and assets from internal and external threats, to provide for the basic objectives of protection and defense, and to preserve the confidentiality, integrity, and availability of information.

This policy aims to comply with the necessities of cybersecurity and the related legislative and regulatory requirements, namely the legal obligations outlined in No. 2-1-3 of the Essential CyberSecurity Controls (ECC-1:2018) issued by the National CyberSecurity Authority.

نطاق العمل وقابلية التطبيق

Scope and Applicability of the Work

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الملك عبد العزيز، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) والطلاب في جامعة الملك عبد العزيز.

This policy covers all information and technology assets pertaining to King AbdulAziz University, and it applies to all personnel (employees and contractors) and students at King AbdulAziz University.

بنود السياسة

Policy Clauses

١- البنود العامة

١-١ يجب اتباع متطلبات الأمن السيبراني في السياسات والمعايير والإجراءات المعتمدة لدى جامعة الملك عبد العزيز.

١-٢ يجب حماية البيانات، والأصول (الأجهزة أو المعلومات أو البرامج) والتعامل معها حسب حساسيتها وتصنيفها، وفقاً لسياسة حماية البيانات المعتمدة لدى جامعة الملك عبد العزيز وضمان سرية البيانات وسلامتها وتصنيفها وتوافرها.

1- General requirements

1-1 Cybersecurity requirements must be met in the policies, standards and procedures approved by King AbdulAziz University.

1-2 Data and assets (hardware, information, or software) must be protected and handled as per their sensitivity and classification in accordance with the Data Protection Policy approved by King AbdulAziz University. Also, data

confidentiality, integrity and availability must be ensured.

1-3 No printed matters should be left unattended on the shared printer.

1-4 External storage media must be kept in a secure and appropriate manner, such as ensuring that the temperature is set at a certain degree and stored in an insulated and safe place.

1-5 It is prohibited to disclose any of the King AbdulAziz University information, including systems and networks related information, to any unauthorized entity or party, whether internal or external.

1-6 It is prohibited to publish information about the King AbdulAziz University via the media and social media networks without permission of the Authorizing Official.

1-7 It is prohibited to use the King AbdulAziz University systems and assets to achieve personal benefit and business, or for any purpose not related to the activity and works of university.

1-8 It is prohibited to connect personal devices to networks and systems of King AbdulAziz University without prior authorization from the Cyber security Center. This should be done in accordance with Workstations, Mobile Devices and BYOD Security Policy approved by the university.

1-9 It is prohibited to perform any activities intended to bypass the King AbdulAziz University protection systems, including anti-virus programs, firewall, and malware without prior authorization, and in accordance with the procedures approved by the university.

1-10 The CyberSecurity Center retains its right to monitor and periodically review work-

١-٣ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

١-٤ يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

١-٥ يمنع الإفصاح عن أي معلومات تخص جامعة الملك عبد العزيز، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

١-٦ يُمنع نشر معلومات تخص جامعة الملك عبد العزيز عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

١-٧ يُمنع استخدام أنظمة جامعة الملك عبد العزيز وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الجامعة

١-٨ يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة الملك عبد العزيز دون الحصول على تصريح مسبق من مركز الامن السيبراني، وبما يتوافق مع سياسة أمن اجهزة المستخدمين والاجهزة المحمولة (BYOD) والأجهزة الشخصية المعتمدة لدى الجامعة.

١-٩ يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بجامعة الملك عبد العزيز، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة الملك عبد العزيز.

١-١٠ يحتفظ مركز الأمن السيبراني بحقه في مراقبة الأنظمة والشبكات والأجهزة الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات ومعايير الأمن السيبراني لدى جامعة الملك عبد العزيز.

١-١١ يجب أن تكون البطاقة التعريفية للموظفين و الزوار بارزة في جميع مرافق جامعة الملك عبد العزيز.

١-١٢ يجب تبليغ مركز الأمن السيبراني في حال فقدان المعلومات الخاصة بجامعة الملك عبد العزيز أو سرقتها أو تسريبها.

١-١٣ يجب متابعة قواعد الاستخدام المقبول للمعلومات والأصول المرتبطة بأنظمة معالجة المعلومات.

related systems, networks and personal devices, in order to monitor compliance with cybersecurity policies and standards approved by King AbdulAziz University.

1-11 The identification card of employees and visitors must visible in all facilities of King AbdulAziz University.

1-12 The CyberSecurity Center must be notified in case of loss, theft or leakage of King AbdulAziz University information.

1-13 Information and Asset Acceptable Use rules related to Information Processing systems must be followed up.

1-14 All King AbdulAziz University employees and staff must return all files, documents, information and assets in their possession upon work completion or expiry of their contract/agreement.

1-15 It is prohibited to transfer assets off-site without prior permission from relevant departments.

1-16 Assets that are off-site must be protected taking into account the various risks of working outside King AbdulAziz University buildings.

1-17 Sessions, meetings and contents related to security awareness campaigns organized by the King AbdulAziz University must be attended and should be abided by.

1-18 All staff must sign a statement of consent on Asset Acceptable Use approved by King AbdulAziz University.

1-19 All staff must approve and acknowledge the Code of Conduct and Acceptable Use Policy upon any review or update thereof.

1-20 Access to King AbdulAziz University assets must be according to roles and

١-١٤ يجب على جميع الموظفين والعاملين في جامعة الملك عبد العزيز إرجاع جميع الملفات والمستندات والمعلومات والأصول التي في حوزتهم عند إنهاء عملهم أو عقدهم، أو اتفاقهم.

١-١٥ يُمنع نقل الأصول خارج مواقعها بدون إذن مسبق من الإدارات المعنية.

١-١٦ يجب حماية الأصول التي تكون خارج المواقع مع مراعاة المخاطر المختلفة للعمل خارج مباني جامعة الملك عبد العزيز.

١-١٧ يجب حضور الجلسات واللقاءات والمحتويات الخاصة بحملات التوعية الأمنية التي تقدمها جامعة الملك عبد العزيز والالتزام بها.

١-١٨ يجب على جميع العاملين توقيع إقرار الموافقة على الاستخدام المقبول للأصول المعتمدة لدى جامعة الملك عبد العزيز.

١-١٩ يجب على جميع العاملين الموافقة والإقرار على قواعد السلوك وسياسة الاستخدام المقبول عند أي مراجعة أو تحديث عليها.

١-٢٠ يجب أن يكون الوصول الى اصول جامعة الملك عبد العزيز وفقا للمسؤوليات والادوار المطلوبة لأداء المهام فقط.

١-٢١ يجب تنبيه مشرفي الأصول التقنية حول تصحيحات الأمن السيبراني التي يجب تطبيقها وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى جامعة الملك عبد العزيز.

١-٢٢ يجب على ملاك الأصول مراجعة صلاحيات وصول المستخدمين على فترات محددة ومنتظمة.

١-٢٣ يجب تبليغ مركز الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على جامعة الملك عبد العزيز أو أصولها مثل: وجود مواقع مشبوهة، الاشتباه بوجود مخاطر سيبرانية أو الاشتباه بمحتوى بريد الكتروني قد يتسبب بضرر للجامعة.

١-٢٤ في حال عدم الالتزام بأحد البنود يجب على الجامعة تقديم مبررات للهيئة الوطنية للأمن السيبراني وذكر أسباب عدم الالتزام.

١-٢٥ يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

responsibilities required to perform tasks only.

1-21 Technical asset administrators must be alerted about cybersecurity patches to be implemented according to King AbdulAziz University Patch Management Policy.

1-22 Asset owners must review user access rights at defined and regular intervals.

1-23 The CyberSecurity Center must be notified when suspecting any activity that may harm King AbdulAziz University or its assets, such as suspected sites, cybersecurity risks or mail contents that may harm university.

1-24 In case of non-compliance with any item, King AbdulAziz University must explain and state the reasons for National Cybersecurity Authority.

1-25 Allowing unauthorized persons to enter sensitive areas without obtaining prior permission is prohibited.

1-26 Key performance indicators (KPIs) must be used to ensure correct and effective use of requirements and protect King AbdulAziz University information and technology assets.

2- Protection of Laptops

2-1 It is prohibited to use external storage media without prior authorization from the CyberSecurity Center. When used, stored data must be encrypted according to the King AbdulAziz University Encryption Standard.

2-2 Devices must be secured before leaving office by Sign out or Lock, whether leaving for a short time or after working hours.

2-3 It is prohibited to use or install hardware, tools, or applications unapproved by King

١-٢٦ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأصول المعلوماتية والتقنية الخاصة بالجامعة.

٢- حماية أجهزة الحاسب الآلي

١-٢ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من مركز الأمن السيبراني. وعند الاستخدام يجب تشفير البيانات المخزنة عليها وفقا لمعيار التشفير المعتمد لدى الجامعة.

٢-٢ 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.

٣-٢ يُمنع استخدام أو تثبيت أجهزة أو أدوات أو تطبيقات غير معتمدة من جامعة الملك عبد العزيز على جهاز الحاسب الآلي دون الحصول على إذن مسبق من الإدارة العامة لتقنية المعلومات.

٤-٢ يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من مركز الأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

٥-٢ يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٣- الاستخدام المقبول للإنترنت والبرمجيات

١-٣ يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية وعدم التفاعل معها إلا بالتواصل مع مركز الامن السيبراني.

٢-٣ يُمنع انتهاك حقوق أي شخص، او 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 لأي غرض من أغراض العمل، أو استخدام وسائط تخزين خارجية بدون أخذ الموافقة من الجامعة.

AbdulAziz University on the laptop without prior authorization of General Administration of Information Technology.

2-4 It is likewise prohibited to engage in any activity that affects the efficiency and security of university systems and assets without obtaining prior permission from the CyberSecurity Center, including activities that enable users to gain enhanced powers and privileges.

2-5 It is forbidden to leave any and all classified information in easily-accessible places, or to allow such information to be viewed by unauthorized persons

3- Internet and Software Acceptable Use

3-1 Security messages that may arise while browsing the internet or internal networks must be treated cautiously and be dealt with only after contacting CyberSecurity Center.

3-2 It is prohibited to violate the rights of any person, or company protected by copyright, patent or other intellectual property, similar laws or regulations, including, but not limited to, installation of unauthorized or illegal software for any business purposes, or use of external storage media without consent of King AbdulAziz University.

3-3 A secure and authorized browser must be used to access internal network or the internet.

3-4 It is prohibited to use techniques that allow bypassing Proxy or Firewall to access the Internet.

3-5 It is prohibited to upload or install Software and tools on King AbdulAziz University assets without prior authorization of General Administration of Information Technology.

٣-٣ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٣-٤ يُمنع استخدام التقنيات التي تسمح بتجاوز الخادم الوكيل (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٣-٥ يُمنع تحميل البرمجيات والأدوات أو تثبيتها على أصول جامعة الملك عبد العزيز دون الحصول على تصريح مسبق من الإدارة العامة لتقنية المعلومات.

٣-٦ يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات دون الحصول على تصريح مسبق من مركز الامن السيبراني.

٣-٧ يُمنع إجراء أي فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة الملك عبد العزيز وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من مركز الأمن السيبراني.

٣-٨ يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

٤- الاستخدام المقبول للبريد الإلكتروني

٤-١ يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس الإلكتروني في غير أغراض العمل، ويكون الاستخدام بما يتوافق مع سياسات الأمن السيبراني ومعاييره المعتمدة لدى جامعة المك عبد العزيز.

٤-٢ يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

٤-٣ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات وفقاً لسياسة حماية البيانات المعتمدة لدى جامعة الملك عبد العزيز.

٤-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بجامعة الملك عبد العزيز في أي موقع ليس له علاقة بالعمل.

3-6 It is prohibited to use Internet for non-business purposes, including uploading media and files, as well as using file sharing software without prior authorization of CyberSecurity Center.

3-7 It is prohibited to conduct a security check to discover security vulnerabilities, including penetration testing, or monitoring networks and systems, or third-party networks and systems without prior authorization of CyberSecurity Center.

3-8 It is forbidden to visit suspicious sites, including those that provide hacking instructions.

4- Email Acceptable Use

4-1 It is prohibited to use email, telephone or e-fax for non-business purposes, noting that their use shall only be in accordance with cybersecurity policies and standards approved by King AbdulAziz University.

4-2 It is prohibited to exchange messages containing inappropriate or unacceptable content, including messages with internal and external parties.

4-3 Encryption techniques must be used when sending sensitive information via email or communication systems as per the King AbdulAziz University Data Protection Policy.

4-4 King AbdulAziz University e-mail addresses should not be used to register with any website that is not work-related.

4-5 King AbdulAziz University has the right to disclose emails' content after obtaining the necessary permits from the Representative and the Cybersecurity Center in accordance with the King

٥-٤ تحتفظ جامعة الملك عبد العزيز بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية ومركز الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة لدى جامعة الملك عبد العزيز.

٦-٤ يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٥- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

١-٥ يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية تتعلق بالعمل.

٢-٥ يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق باستخدام أدوات أو برمجيات خاصة بجامعة الملك عبد العزيز.

٣-٥ يُمنع عقد اجتماعات تتعلق بالعمل في أماكن عامة لخطورة تسريب معلومات مصنفة.

٦- استخدام كلمات المرور

١-٦ يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة الملك عبد العزيز وأصولها وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعة الملك عبد العزيز. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٢-٦ 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 العامة لتقنية المعلومات وإبلاغ مركز الامن السيبراني فوراً في حال وقوع ذلك.

٣-٦ يجب تغيير كلمة المرور بشكل دوري حسب سياسة كلمة المرور أو عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

AbdulAziz University's relevant approved procedures and regulations.

4-6 It is prohibited to open suspicious or unexpected emails and attachments, even if they appear to be from reliable sources.

5- Video Conferences and Web-Based Communications

5-1 It is prohibited to use unauthorized tools or software to make calls or hold video conferences related to work.

5-2 It is prohibited to make calls or hold video conferences not related to work without prior authorization to use King AbdulAziz University 's tools or software.

5-3 It is prohibited to hold work-related meetings in public places due to the risk of leaking classified information.

6- Passwords Use

6-1 It is necessary to choose secure passwords and to safeguard King AbdulAziz University systems and assets passwords in accordance with King AbdulAziz University's Identity and Access Management Policy. It is also necessary to choose passwords different from those of personal accounts, such as personal mail and social media accounts.

6-2 It is forbidden to share passwords by any means, including electronic messages, voice communication, and writing on paper. All users must never disclose their passwords to any party, including co-workers and the staff of the General Administration of Information Technology.

6-3 It is required to periodically change your password and in the event that a new password is provided to you by the

٦-٤ يمنع استخدام كلمات مرور مستخدمة من قبل أو متعارف عليها، بالإضافة إلى عدم مشاركة كلمة المرور الخاصة بالمستخدم لأي شخص إطلاقًا.

٧- استخدام المكتب

٧-١ يجب الالتزام بسياسة المكتب الآمن والنظيف المعتمدة لدى جامعة الملك عبد العزيز، والتأكد من خلو سطح المكتب وشاشة العرض من المعلومات المصنفة والحساسة وفقًا للتصنيفات المعتمدة لدى الجامعة.

٧-٢ يُمنع ترك أي معلومات مصنفة أو حساسة بالنسبة لجامعة الملك عبد العزيز في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٧-٣ يُمنع ترك أبواب المكتب والخزانات التي تحتوي على معلومات مصنفة وحساسة مفتوحة.

٨- الحوسبة السحابية

٨-١ يجب تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند انتهاء الخدمة.

٨-٢ يجب فصل البيئة الخاصة بجامعة الملك عبد العزيز (وخصوصًا الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.

٨-٣ يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية بيانات ومعلومات المشتركين في الحوسبة السحابية وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، بحد أدنى ما يلي:

- وجود ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة مع مقدم الخدمة (Exit Strategy).
- استخدام وسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.

system administrator according to King AbdulAziz University Password Policies.

6-4 It is prohibited to use previously used or common passwords. It is also prohibited to share user's password with anyone.

7- Office Use:

7-1 It is necessary to abide by King AbdulAziz University 's Secure and Clean Office Policy, and to make sure the desktop and screen are free of classified and sensitive information as per university 's approved classifications.

7-2 It is prohibited to leave any King AbdulAziz University classified or sensitive information in places that are easily accessible, or accessed by unauthorized persons.

7-3 Office doors and cabinets containing classified and sensitive information must not be left open.

8- Cloud Computing

8-1 Data must be classified prior to being hosted with cloud computing and hosting service providers, and returned to the organization (in a usable format) upon service completion.

8-2 King AbdulAziz University environment (especially virtual servers) must be separated from other cloud computing environment of other organizations.

8-3Cybersecurity requirements for protecting the data and information of cloud computing subscribers must cover, at a minimum, the following:

- Guarantees for ability to delete data safely upon expiry of relationship with service provider (Exit Strategy).
- Use secure means to export and transfer data and virtual infrastructure.

الأدوار والمسؤوليات

Roles and Responsibilities

١- **مالك السياسة :**مدير مركز الأمن السيبراني
٢- **مراجعة السياسة وتحديثها :**مركز الأمن السيبراني
٣- **تنفيذ السياسة وتطبيقها :**الإدارة العامة للموارد البشرية
٤- **قياس الالتزام بالسياسة :**مركز الأمن السيبراني

1- **Policy Owner:** Director of the CyberSecurity Center.
2- **Updating and Reviewing of the Policy:** The CyberSecurity Center.
3- **Implementation and Application of the Policy:** The General Administration of Human Resources.
4- **Measuring Policy Compliance:** CyberSecurity Center.

الالتزام بالسياسة

Compliance with the Policy

١- يجب على مدير مركز الأمن السيبراني التأكد من التزام جامعة الملك عبد العزيز بهذه السياسة دوريًا.

٢- يجب على كافة العاملين في جامعة الملك عبد العزيز الالتزام بهذه السياسة.

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الملك عبد العزيز.

1- The Director of CyberSecurity Center must ensure that the university complies with this policy periodically.

2- All employees of the university must comply with this policy.

3- Any violation of this policy may subject the offender to disciplinary action, in accordance with the university's Supervisory Committee for CyberSecurity.

معايير الاستثناء

Waiver Criteria

يمكن التقدم بطلبات الحصول على استثناءات من هذه السياسة رسمياً إلى مركز الأمن السيبراني مع توضيح مسوغات الاستثناء، والمزايا التي قد تنجم عنه، على أن يتم الموافقة عليها من اللجنة الإشرافية للأمن السيبراني. تمتد فترة الاستثناء من السياسة لمدة عام واحد كحد أقصى قابلة للتجديد، على ألا يتم منح استثناء لمدة تزيد عن ٣ فترات متعاقبة.

Waivers from this policy could be formally submitted to the CyberSecurity Center, including justification and benefits attributed to the waiver, and must be approved by the Supervisory Committee for cybersecurity. The policy waiver period has maximum period of one year, and can be reassessed and re-approved, for maximum 3 consecutive terms.

التحديث والمراجعة

Update and Review

يجب على مركز الأمن السيبراني مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة الملك عبد العزيز أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

The CyberSecurity Center must review the policy at least annually or whenever there are changes in the policies or organizational procedures of King AbdulAziz University or related legislative and regulatory requirement