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

Acceptable Use Policy for Assets

CSC-Pol-02
Version 2.1 الإصدار
01/01/2024

التصنيف: عام
Classification: General

قائمة المحتويات

الاهداف ٣
نطاق العمل وقابلية التطبيق ٣
بنود السياسة ٣
الالتزام بالسياسة ٨
معايير الاستثناء ٨

INDEX

Objectives 3
Scope and Applicability of the Work 3
Policy Clauses 3
Compliance with the Policy 8
Waiver Criteria 8

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 والطلاب في جامعة الملك عبد العزيز.

This policy covers all information and technology assets pertaining to King Abdulaziz University, and it applies to all members of staffs 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.

٢-١ يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بجامعة الملك عبد العزيز بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

٣-١ يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

1- General Clauses

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

1-2 All information must be handled in accordance with its defined classification, and in accordance with the data classification policy and the data and information security policy of King Abdulaziz University, in a way that ensures that the confidentiality, integrity, and availability of information are preserved.

1-3 Infringement upon the rights of any person or company protected by copyrights or patents, or upon any other item of intellectual property, or upon analogous laws and regulations, including but not limited to the downloading of illegal or unauthorized software, for example, is prohibited.

1-4 Printouts made using shared printers must not be left unattended.

1-5 External storage devices must be kept safe and secure, for example by ensuring that room temperatures are set at appropriate degrees, and by storing such devices in isolated and secure places.

1-6 The use of passwords belonging to other members of staff is prohibited, including passwords belonging to one's managers or subordinates.

1-7 Adherence to a secure clean desk policy is required. Staff must ensure that desktop and display screens are free of classified information.

1-8 Disclosure of any and all information pertaining to King Abdulaziz University, including information relating to systems and networks, to any agency or party, whether internal or external, is prohibited.

1-9 Publication of information pertaining to King Abdulaziz University through media channels or social communications networks without prior permission is prohibited.

1-10 Use of King Abdulaziz University systems and assets for the purpose of personal benefit or business, or for any purpose not relating to the activity and work of King Abdulaziz University, is prohibited.

1-11 Connection of personal devices to King Abdulaziz University networks and systems without obtaining prior authorization is prohibited. Personal devices connected to the university networks must be in accordance with the Mobile Device Security Policy (BYOD).

1-12 It is prohibited to engage in any and all activities aimed at bypassing King Abdulaziz University security systems, including the use of anti-virus programs, firewalls, and harmful software, without obtaining prior authorization. Such activities must be carried out in accordance with the procedures authorized by King Abdulaziz University.

1-13 The CyberSecurity Center reserves its right to monitor and periodically review work-related personal systems, networks, and accounts in order to monitor compliance with cybersecurity policies and standards.

١-٤ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

١-٥ يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

١-٦ يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

١-٧ يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

١-٨ 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.

١-٩ يُمنع نشر معلومات تخص جامعة الملك عبد العزيز عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

١-١٠ يُمنع استخدام أنظمة جامعة الملك عبد العزيز وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة الملك عبد العزيز.

١-١١ يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة الملك عبد العزيز دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

١-١٢ 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.

١-١٣ تحتفظ مركز الأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

1-14 Allowing unauthorized persons to enter sensitive areas without obtaining prior permission is prohibited.

1-15 Identification cards must be worn when inside any and all King Abdulaziz University facilities.

1-16 The CyberSecurity Center must be notified in the event of any loss, theft, or leak of information.

1-17 All university employees and workers must return all files, documents, information, technical, and non-technical assets in their possession upon termination of their work or contract, and not leave any of them in their possession.

1-18 It is prohibited to move assets outside their locations without prior permission from the concerned departments.

1-19 Attending and adhering to the sessions, meetings, and contents of security awareness campaigns provided by King Abdulaziz University is mandatory for all employees.

1-20 All employees must sign a declaration of approval for the acceptable use of assets approved by King Abdulaziz University.

2- Computer and Data Security

2-1 Use of external storage media without obtaining prior permission from the CyberSecurity Center is prohibited.

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

2-3 Staff members' devices must be secured, either by locking device screens or by signing out, prior to leaving the office, whether for a short time or at the end of the working day.

2-4 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.

2-5 Installation of external applications on computers without prior permission from the General Administration of Information Technology is prohibited.

١-١٤ يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

١-١٥ يجب ارتداء البطاقة التعريفية في جميع مرافق جامعة الملك عبد العزيز.

١-١٦ يجب تبليغ مركز الأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

١-١٧ يجب على جميع الموظفين والعاملين في الجامعة إرجاع جميع الملفات والمستندات والمعلومات والأصول التقنية والغير تقنية التي في حوزتهم عند إنهاء عملهم أو عقدهم، وعدم ترك أى منهم في حوزتهم.

١-١٨ يمنع نقل الأصول خارج مواقعها بدون إذن مسبق من الإدارات المعنية.

١-١٩ يجب حضور الجلسات واللقاءات والمحتويات الخاصة بحملات التوعية الأمنية التي تقدمها الجامعة والإلتزام بها.

١-٢٠ يجب على جميع العاملين توقيع إقرار الموافقة على الإستخدام المقبول للأصول المعتمدة لدى الجامعة.

٢- حماية أجهزة الحاسب الآلي والبيانات

٢-١ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من مركز الأمن السيبراني.

٢-٢ 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.

٢-٣ 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.

٢-٤ يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٢-٥ يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من الإدارة العامة لتقنية المعلومات.

2-6 Upon suspicion of any activity that may cause harm to computers or assets pertaining to King Abdulaziz University, notification of the CyberSecurity Center is required.

3- Acceptable Use of the Internet and Software

3-1 The CyberSecurity Center must be notified of suspicious websites that should be blocked, or vice versa.

3-2 It is necessary to ensure that intellectual property rights are not violated when downloading information or documents for work purposes.

3-3 Use of unlicensed software or other kinds of intellectual property is prohibited.

3-4 Use of a secure and authorized browser to access both the internal University network and the Internet is required.

3-5 Use of technologies that allow for proxies and firewalls to be bypassed in accessing the Internet is prohibited.

3-6 It is forbidden to download or install software and applications to King Abdulaziz University assets without obtaining prior permission from the General Administration of Information Technology.

3-7 Use of the Internet for non-work-related purposes, including the downloading of media and files and the use of file-sharing software, is prohibited.

3-8 Notification of the CyberSecurity Center when cybersecurity risks are suspected is required. Circumspection should be used when dealing with security messages that appear while surfing the Internet or the internal University network.

3-9 It is forbidden to conduct security tests for the purpose of discovering security vulnerabilities, including penetration tests, or to monitor King Abdulaziz University networks and systems or the networks and systems of parties external to the University, without obtaining prior permission from the CyberSecurity Center.

3-10 The location for hosting and storing information related to and owned by King Abdulaziz University must be within the Kingdom, and storage must be in accordance with the relevant legislative and regulatory requirements.

٦-٢ يجب تبليغ مركز الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بجامعة الملك عبد العزيز أو أصولها.

٣- الاستخدام المقبول للإنترنت والبرمجيات

١-٣ يجب إبلاغ مركز الأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

٢-٣ يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

٣-٣ يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

٤-٣ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٥-٣ يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٦-٣ يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة الملك عبد العزيز دون الحصول على تصريح مسبق من الإدارة العامة لتقنية المعلومات.

٧-٣ يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

٨-٣ يجب تبليغ مركز الأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

٩-٣ يُمنع إجراء 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.

١٠-٣ يجب أن يكون موقع استضافة وتخزين معلومات العمل داخل المملكة، وأن يكون التخزين وفقًا للمتطلبات التشريعية والتنظيمية ذات العالقة.

3-11 It is forbidden to visit suspicious sites, including those that provide hacking instructions.

4- Acceptable Use of E-Mail and Communications Systems

4-1 It is forbidden to use e-mail, telephones, fax machines, or e-fax systems for non-work-related purposes. Such devices must be used in accordance with cybersecurity policies and standards.

4-2 It is forbidden to circulate messages containing inappropriate or unacceptable content, including messages circulated among either internal or external parties.

4-3 The use of encryption technologies when sending sensitive information by means of e-mail or communication systems is required.

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

4-5 It is necessary to notify the CyberSecurity Center when the presence of e-mail messages containing content that may cause harm to King Abdulaziz University systems or assets is suspected.

4-6 King Abdulaziz University reserves the right to disclose the contents of e-mails, after obtaining the necessary permissions from the competent authorities and the CyberSecurity Center, in accordance with the relevant procedures and regulations.

4-7 It is forbidden to open suspicious or unusual emails or attachments, even if they appear to originate from reliable sources.

5- Video Meetings and Web-Based Communications

5-1 The use of unauthorized applications or software for engaging in communications or holding video meetings is prohibited.

5-2 Engaging in non-work-related communications or holding non-work-related video meetings without obtaining prior permission is prohibited.

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

١١-٣ يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

٤- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

١-٤ يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

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

٣-٤ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

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

٥-٤ يجب تبليغ مركز الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة الملك عبد العزيز أو أصولها.

٦-٤ 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.

٧-٤ 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.

٢-٥ يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

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

6- Use of Passwords

6-1 It is necessary to select and preserve secure passwords for King Abdulaziz University systems and assets. It is also necessary to select passwords that are different from those used for personal accounts, such as e-mail accounts and accounts on social communications websites.

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 system administrator according to King Abdulaziz University Password Policies.

٦- استخدام كلمات المرور

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

٦-٢ 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.

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

Compliance with the Policy

الالتزام بالسياسة

1- The 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.

١- يجب على مركز الأمن السيبراني ضمان إلتزام الجامعة بهذه السياسة دورياً.
٢- يجب على كافة العاملين في الجامعة الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب توصيات اللجنة الإشرافية للأمن السيبراني بالجامعة.

Waiver Criteria

معايير الاستثناء

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.

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.