التحكم في الوصول سياسة

IKVKK_P7الإصدار 1.00

شركة كارديلين المحدودة لتجارة صناعة الدهانات والمواد الكيميائية

سياسة التحكم في الوصول

.1الغرض والنطاق

تقوم شركة Kardelen Boyaبتطبيق ضوابط الوصول المادية والمنطقية على الشبكات وأنظمة تكنولوجيا المعلومات والخدمات التي تستخدمها الشركة لتوفير وصول مفصل وقابل للتدقيق ومناسب للمستخدم، مع تعديل مستويات التفويض لتناسب الخدمة المقدمة، ولضمان والحفاظ على سرية البيانات وسلامتها وتوافرها وفقًا لسياسة أمن المعلومات الخاصة بها.

يهدف التحكم في الوصول إلى حماية مصالح جميع المستخدمين المصرح لهم لأنظمة تكنولوجيا المعلومات التي تستخدمها شركة Kardelen Boya، بالإضافة إلى البيانات المقدمة من أطراف ثالثة، من خلال إنشاء بيئة عمل آمنة ومأمونة ويمكن الوصول إليها.

.1.1تسري هذه السياسة على جميع البيانات والمعلومات والأنظمة التي تملكها أو تشغلها شركة كارديلين بويا في جميع المواقع التي يُتاح فيها الوصول إلى أنظمة تكنولوجيا المعلومات والاتصالات الإلكترونية التي تستخدمها الشركة. كما تسري أحكام هذه السياسة على جميع الموردين والمقاولين والمقاولين من الباطن والمستشارين والمتطوعين والموظفين المرافقين للدراسات البحثية والطلاب المتدربين والعمال المؤقتين، بما في ذلك الأطراف الثالثة والمؤسسات المصرح لها بالوصول إلى أنظمة تكنولوجيا المعلومات والاتصالات الإلكترونية الخاصة بشركة كارديلين بويا. ويشمل مصطلحا "مستخدم أصول المعلومات" أو "المستخدم" المستخدمان في هذه السياسة الفئات المذكورة آنفًا من الأفراد.

.1.2موقع الشركة الإلكتروني المتاح للجمهور والمعلومات الأخرى المصنفة على أنها "متاحة للجمهور".
لا يشمل هذا البيان الأنظمة الخارجة عن سيطرة شركة كارديلين بويا. تقع مسؤولية منح صلاحيات الوصول إلى الأنظمة والموارد والتطبيقات غير الخاضعة لإدارة الشركة على عاتق مالك النظام أو المورد أو التطبيق، وليس على عاتق كارديلين بويا. كما تقع مسؤولية عمليات الترخيص والتحكم المتعلقة بمنح الوصول إلى هذه الموارد على عاتق مالكي الموارد.

.2تعريفات وأدوار المشاركين

.2.1لا يُسمح بالوصول إلى البيانات والمعلومات والأنظمة إلا عند ظهور ضرورة تجارية مشروعة.
لا يُمنح الوصول إلا إذا أذن مالك أصول المعلومات بذلك، وتم الالتزام بجميع السياسات والإجراءات والمبادئ والشروط المعمول بها. إذا لم يعد المستخدم بحاجة إلى الوصول إلى النظام لأسباب مثل تغيير الوظيفة، أو التقاعد، أو إنهاء الخدمة، أو إتمام المشروع، فيجب إلغاء جميع صلاحيات الوصول المحددة، وإنهاء حقه في الوصول إلى المعلومات.

.2.2تسمح امتيازات المستخدم للمستخدمين بالوصول إلى الأنشطة المحددة للمستخدمين الآخرين.
أو يجب تعريفها بطريقة تمنع صاحب المعلومات من الوصول إلى أي بيانات لم يصرح المستخدم المعني بالوصول إليها بشكل محدد، أو التدخل فيها بأي شكل من الأشكال.

2.3.سيتم منح حقوق الوصول إلى كل من الكيانات المادية والمنطقية وفقًا لمبادئ أقل حقوق الوصول والحاجة إلى المعرفة.

2.4.مبدأ أقل قدر من الوصول يعني أن المستخدم المحدد لا يحق له إلا الحقوق الممنوحة له.
يتطلب هذا ألا يمتلك المستخدم صلاحيات وصول تتجاوز ما هو ضروري لأداء مهامه ومسؤولياته. ولتطبيق مبدأ الحد الأدنى من صلاحيات الوصول بفعالية، يجب تحديد طبيعة عمل المستخدم، وتحديد الحد الأدنى من صلاحيات الوصول اللازمة لإنجاز المهمة، وتقييد صلاحيات الوصول الممنوحة للمستخدم بما يتوافق مع هذا الحد الأدنى.

ستخضع أذونات التحكم في الوصول لجميع الأنظمة لإعداد افتراضي يمنع المستخدمين غير المصرح لهم من الوصول إليها، وسيتم تطبيق مبدأ الوصول بأقل الامتيازات، مما يتطلب حظر أي امتياز لنظام المعلومات غير مسموح به على وجه التحديد.

2.5.يشير مبدأ الأمن المتعمق إلى تطبيق دفاع أمني عبر طبقات متعددة من أنواع مختلفة لتوفير حماية أفضل بشكل ملحوظ. سيتم تطبيق مبدأ الأمن المتعمق، مما يتطلب التحكم في الوصول على كل طبقة من طبقات النظام، بما في ذلك الشبكة، والأجهزة، وبرامج النظام، والتطبيقات، والبيانات.

2.6.فصل المهام: إذا تضمنت عملية تجارية معالجة معلومات أساسية أو بالغة الأهمية للشركة، فيجب أن يتضمن النظام فصلًا للمهام أو آليات تحكم تعويضية أخرى للمستخدمين. ينبغي أن تضمن هذه الآليات عدم امتلاك أي شخص سلطة حصرية على أصول المعلومات أو الوظائف ذات الصلة. ومن أمثلة انتهاك مبدأ فصل المهام أن يكون الشخص نفسه مسؤولاً عن كتابة الشيكات والاحتفاظ بالبيانات التاريخية المتعلقة بالمعاملات المالية.

كلما أمكن، لا ينبغي أن يكون أي شخص مسؤولاً بمفرده عن إنجاز مهمة تتضمن معلومات خاصة أو حساسة أو بالغة الأهمية من البداية إلى النهاية. وبالمثل، لا ينبغي أن يكون أي شخص مسؤولاً عن الموافقة على عمله. وحيثما كان ذلك ممكناً، ينبغي أن ينسق شخصان على الأقل أنشطة معالجة المعلومات لكل مهمة.

2.7.الاستخدام المقبول: Kardelenقبل تحديد اسم المستخدم وكلمة المرور.
يجب إبلاغ كل مستخدم يرغب في الحصول على إذن للاتصال بالأنظمة التي تستخدمها شركة بويا بسياسة الاستخدام المقبول لموارد تكنولوجيا المعلومات والاتصالات الإلكترونية، ويجب عليه التوقيع على إعلان الوعي بأمن المعلومات.

2.8.يلتزم جميع الأطراف الثالثة التي لديها إمكانية الوصول إلى بيانات الشركة ومعلوماتها وأنظمتها بالامتناع عن إفشاء أي معلومات تعتبرها شركة كارديلين بويا غير متاحة للعموم. بالنسبة للأطراف الثالثة المتعاقدة بموجب عقد أو أمر شراء أو اتفاقية تعاقد من الباطن، سيتم تضمين بند سرية قياسي في جميع العقود وأوامر الشراء المبرمة بين كارديلين بويا والطرف الثالث الممنوح له حق الوصول إلى بيانات كارديلين بويا ومعلوماتها وأنظمتها. كما سيتم إبرام اتفاقية سرية مكتوبة لجميع الأفراد أو المؤسسات التي تقدم خدمات لكارديلين بويا (مما يتطلب الوصول إلى بيانات سرية) ولكن ليس لديها عقد مع كارديلين بويا.

2.9.التحكم في الوصول: يشير التحكم في الوصول إلى أي آلية تتيح الوصول إلى البيانات. للوصول إلى أجهزة الكمبيوتر، يجب على المستخدم أولاً تسجيل الدخول باستخدام طريقة مصادقة مناسبة. تقارن آلية التحكم في الوصول اسم المستخدم المخصص للمستخدم بقائمة التحكم في الوصول.

يتحكم النظام في المهام والعمليات التي يمكن للمستخدم المعني القيام بها والتي لا يمكنه القيام بها.

تتضمن أنظمة التحكم في الوصول العناصر التالية: •إنشاء الملفات أو قراءتها أو تحريرها أو حذفها على خادم الملفات، وما إلى ذلك.

أذونات الملفات

•برامج مثل الحق في تشغيل برنامج معين على خادم التطبيقات.

الأذونات

•حقوق البيانات، مثل استرجاع البيانات من قاعدة البيانات أو تحديث المعلومات.

تشير إجراءات التحكم في الوصول إلى مجمل الأساليب والممارسات التي يستخدمها مالكو أصول المعلومات لتخويل المستخدمين بالوصول إلى البيانات أو المعلومات أو الأنظمة.

2.10. المصادقة: تشير المصادقة إلى عملية التحقق من بيانات اعتماد مستخدم المعلومات من قِبل مالك أصول المعلومات المُخوّل بتحديد هوية ذلك المستخدم. في أنظمة الحاسوب، تتم المصادقة عادةً باستخدام اسم مستخدم وكلمة مرور فريدين، لا يعرفهما إلا مستخدم المعلومات، ويتم تحديدهما خصيصًا له. يجوز للمدير العام السماح باستخدام طرق مصادقة أخرى بناءً على توصية مدير تقنية المعلومات ومستشار اللائحة العامة لحماية البيانات .2.11 .(GDPR)

النظام: يشير النظام إلى مجموعة من موارد المعلومات المترابطة الخاضعة لنفس الرقابة التنظيمية المباشرة والتي تتشارك في وظائف مشتركة. يمكن أن يتكون النظام من أجهزة، أو برامج، أو معلومات، أو بيانات، أو تطبيقات، أو بنية تحتية للاتصالات. أما نظام المؤسسة، فيشير إلى الأنظمة التي تعالج المعلومات لدعم عمليات الأعمال الجارية.

ستخضع الأنظمة المصنفة كأنظمة مؤسسية لمتطلبات أمنية محددة وفقًا لمتطلبات العمل. .2.12

المسؤولية الفردية: كل مستخدم مسؤول بشكل فردي عن الوصول إلى الموارد الإلكترونية التي توفرها وتستخدمها كارديلين بويا.

يتطلب الوصول إلى أنظمة وشبكات الكمبيوتر استخدام بيانات اعتماد كمبيوتر فريدة يتم تعيينها بشكل فردي لكل مستخدم، والمعروفة باسم اسم المستخدم.
لا يُسمح لأي مستخدم لأدوات تكنولوجيا المعلومات الخاصة بشركة كارديلين بويا بالوصول إلا إلى الموارد المصرح له باستخدامها. ويتطلب كل اسم مستخدم استخدام مفتاح ذكي، مشابه لكلمة مرور تسجيل الدخول، للتحقق من هوية المستخدم عند الوصول إلى البيانات أو المعلومات أو النظام. تُعتبر معلومات كلمة المرور سرية، ويجب عدم إفشائها لأي شخص. يتحمل كل مستخدم مسؤولية اتخاذ التدابير الأمنية المعقولة لمنع الاستخدام غير المصرح به لمعلومات كلمة المرور الخاصة به. لمزيد من المعلومات التفصيلية، يُرجى الاطلاع على: لائحة الإجراءات والمبادئ المتعلقة بتحديد كلمات مرور المستخدمين واستخدامها وحمايتها.

2.13. مالكو أصول المعلومات: يتحمل مالكو أصول المعلومات مسؤولية تحديد من يمكنه الوصول إلى الموارد المحمية، وما هي صلاحيات الوصول المحددة (قراءة، تحديث، إلخ). وتتوافق هذه الصلاحيات مع واجبات ومسؤوليات مستخدم المعلومات. يجوز لمالكي أصول المعلومات تفويض بعض مسؤولياتهم الإدارية إلى مرؤوسيهم، لكنهم يظلون في نهاية المطاف مسؤولين عن أصول المعلومات نفسها. .2.14

رؤساء الأقسام: يضطلع رؤساء الأقسام بدورٍ قيادي في ضمان أمن المعلومات في شركة كارديلين بويا. ويحق لهم الوصول إلى النظام نيابةً عن مستخدمي المعلومات عند الحاجة إلى ذلك لإنجاز العمليات التجارية.

هم مسؤولون عن توثيق الطلبات. رؤساء الأقسام مسؤولون عن تعديل و/أو إلغاء صلاحيات وصول المستخدمين في حال حدوث تغييرات في مسؤولياتهم الوظيفية أو في حالة مستخدم المعلومات.

3.إرشادات إجراءات التحكم في الوصول

3.1.ستوفر شركة Kardelen Boyaلجميع موظفيها ومورديها الخارجيين حقوق الوصول المناسبة إلى البيانات التي تتحكم فيها الشركة لضمان قيامهم بمسؤولياتهم الموكلة إليهم بأكثر الطرق فعالية ممكنة.

3.1.1.معرّفات المستخدم العامة: بيانات اعتماد عامة أو جماعية كقاعدة عامة

لا يُسمح بتحديد هوية واستخدام بيانات كرديلين بويا، ولكن قد يُسمح بذلك في ظروف استثنائية إذا كانت هناك آليات تحكم كافية.

3.1.2.في جميع الأحوال، ستكون شركة Kardelen Boyaهي مزود خدمة الإنترنت.

للوفاء بمسؤولياتها القانونية وإنفاذ أحكام سياسة الاستخدام الأمثل للموارد الإلكترونية، يجب أن تكون هويات المستخدمين الذين لديهم معلومات تعريفية خاصة بالشركة قابلة للتحديد. ولا يجوز مطلقاً استخدام هويات المستخدمين العامة للوصول إلى المعلومات السرية أو الحساسة.

3.1.3.الحسابات ذات حقوق الوصول المميزة: سيتم تقييد تعيين حقوق الوصول المميزة، مثل المسؤول المحلي، ومسؤول المجال، والمستخدم المتميز، ووصول المسؤول، للمستخدمين الذين تعتبرهم الإدارة العليا مناسبين، ولا يمكن تحديدها بشكل افتراضي.

3.1.3.1.لا يتم منح الإذن باستخدام هذه الحسابات وتوثيقه صراحةً إلا من قبل المدير العام بناءً على طلب كتابي من مدير كبير (رئيس القسم، نائب المدير العام).

3.1.3.2.ستتخذ الفرق الفنية الاحتياطات اللازمة لمنع منح حقوق تفضيلية لجميع الفرق من أجل منع الخسائر المحتملة في السرية و/أو النزاهة.

3.1.3.3.لا يجوز استخدام الحسابات المميزة للأنشطة الروتينية؛ البرنامج

لا يجوز استخدام هذه التعريفات إلا لتثبيت البرنامج وإعادة تكوين النظام، وليس لاستخدام البرنامج نفسه، إلا إذا كان تشغيله مستحيلاً بطريقة أخرى.

3.1.4.مبدأ الحد الأدنى من الامتيازات وما تحتاج إلى معرفته: سواء المادية أو...

سيتم منح حقوق الوصول إلى الكيانات المنطقية وفقًا لمبادئ أقل امتيازات الوصول وما تحتاج إلى معرفته.

3.2.صلاحيات التحكم في الوصول 3.2.1.حسابات المستخدمين: الوصول إلى موارد وخدمات تكنولوجيا المعلومات التي تستخدمها شركة كرديلين بويا

سيتم منح الوصول عند إدخال حساب المستخدم الأصلي وكلمة مرور معقدة.

3.2.2.تُمنح حسابات المستخدمين بناءً على وجود سجل موظف صالح في أنظمة معلومات الموارد البشرية. أما بالنسبة لأي مستخدم ليس لديه سجل موظف، فيتم منح إذن الوصول من قِبل رئيس القسم. ويقتصر الوصول الافتراضي على الوصول إلى منطقة محددة، ووسيلة تخزين، وحساب بريد إلكتروني.

3.2.3.الوصول إلى المعلومات السرية، والمعلومات ذات الوصول المقيد، والمعلومات المطلوبة للاستخدام داخل وحدة محددة فقط: الأشخاص المصرح لهم الذين يحتاجون إلى الوصول إلى المعلومات ذات الصلة بسبب مسؤوليات العمل أو العمل التي يتم القيام بها وفقًا للقوانين والاتفاقيات ذات الصلة مع الأطراف المعنية.

سيقتصر الوصول إلى المعلومات المذكورة على الموظفين. وسيتم تقييد الوصول إليها باستخدام جدران الحماية، وفصل الشبكات، وإجراءات تسجيل الدخول الآمنة، وقيود قوائم التحكم بالوصول، وغيرها من الضوابط المناسبة. تقع مسؤولية تطبيق قيود الوصول على عاتق رؤساء الوحدات وقسم تقنية المعلومات الذي يعالج المعلومات ذات الصلة، وسيتم ذلك وفقًا لأحكام هذه السياسة. سيتم تطبيق أساليب التحكم بالوصول القائمة على الأدوار لتأمين الوصول إلى جميع الموارد القائمة على الملفات الموجودة في نطاقات الدليل النشط لشركة كارديلين بويا والتي تُدار من خلالها.

3.3. التحقق من الهوية والمصادقة: يجب أن تكون جميع أجهزة الكمبيوتر المتصلة بشبكة كارديلين بويا مزودة بآليات مصادقة، مثل أسماء المستخدمين وكلمات المرور، لتمكين التحكم في الوصول. يجب أن تحتوي الأنظمة متعددة المستخدمين على أسماء مستخدمين وكلمات مرور فريدة لكل مستخدم، بالإضافة إلى آليات لتقييد صلاحيات وصول المستخدمين. سيتم تطبيق أدوات التحكم البرمجية والمادية لمنع الوصول غير المصرح به إلى جميع محطات العمل، بغض النظر عن حالة الوصول إلى الشبكة، وسيتم اعتمادها من قبل مدير تقنية المعلومات.

3.4. يجب على جميع المستخدمين التحقق من هويتهم قبل الوصول إلى أي معلومات أو بيانات أو أنظمة.
يجب اتباع إجراءات التحقق. ولهذا الغرض، سيُطلب اسم مستخدم وكلمة مرور، يتم تحديدهما بشكل فريد لكل مستخدم على حدة، قبل منح الوصول إلى شبكات الشركة الداخلية.

3.5. يجب على المستخدمين الامتناع عن استخدام أسماء المستخدمين وكلمات المرور التي يستخدمونها للوصول إلى موارد النظام والحوسبة التي تستخدمها Kardelen Boya للوصول إلى أنظمة خارج Kardelen Boya، بما في ذلك الحسابات التي يستخدمونها عبر الإنترنت.

3.6. في أنظمة الكمبيوتر المتصلة بالشبكة، يجب أن تعرض شاشة تسجيل دخول المستخدم فقط ما يلي:
سيتضمن النظام معلومات تطلب من المستخدم إدخال اسم المستخدم وكلمة المرور لتسجيل الدخول. لا يجوز مشاركة أي معلومات خاصة بالشركة، مثل معلومات الكمبيوتر أو نظام التشغيل أو إعدادات الشبكة، مع المستخدم قبل تسجيل دخوله بنجاح باستخدام اسم مستخدم وكلمة مرور صحيحين. في حال إدخال أي من خطوات تسجيل الدخول بشكل خاطئ، سيتم إخطار المستخدم فقط بفشل محاولة تسجيل الدخول، دون توضيح سبب المشكلة.

3.7. أسماء المستخدمين الفريدة: يجب أن يكون كل اسم مستخدم فريدًا للمستخدم المُخصص له، ويجب أن يرتبط به فقط. في حال إنهاء صلاحيات وصول المستخدم إلى النظام، لا يجوز إعادة استخدام اسم المستخدم الخاص به مطلقًا. يجب تحديد كل اسم مستخدم وكلمة مرور للاستخدام الحصري لشخص مُحدد. يجوز مشاركة أسماء المستخدمين عبر رسائل البريد الإلكتروني ووسائل التواصل الأخرى، ولكن لا يجوز مشاركة كلمات المرور مع أي شخص، بأي وسيلة كانت. (يتمتع فريق دعم تقنية المعلومات بصلاحيات وصول خاصة به، ولا يحتاج إلى الوصول إلى كلمات مرور المستخدمين).

3.8. إجراءات مصادقة المستخدم: تضمن جميع أنظمة المعلومات المؤسسية أن المستخدمين المصرح لهم فقط هم من يمكنهم استخدام أسماء المستخدمين مع كلمات المرور المحددة أو أساليب التشفير الديناميكي القوية. يتحمل المستخدمون المسؤولية الفردية عن جميع الإجراءات والمعاملات التي تتم في الجلسات المفتوحة باستخدام أسماء المستخدمين وكلمات المرور أو آليات المصادقة الأخرى. يلتزم المستخدمون بتغيير كلمات مرورهم فورًا في حال اكتشافهم أن معلومات تسجيل دخولهم قد تم الكشف عنها أو استخدامها من قبل جهات خارجية. وبالمثل، يتحمل المستخدمون مسؤولية التحكم في الوصول باستخدام معلومات الجلسة.

إذا اشتبه المستخدمون في انتهاك سرية بياناتهم، فعليهم إبلاغ وحدة الخدمات الفنية بقسم تقنية المعلومات فورًا. لا يجوز استخدام أسماء المستخدمين إلا من قبل الموظفين المُخوَّلين. ويُمنع منعًا باتًا على المستخدمين السماح للآخرين باستخدام أسماء المستخدمين الخاصة بهم. كما لا يجوز لهم إجراء أي عمليات أو معاملات باستخدام أسماء المستخدمين المُخصَّصة لمستخدمين آخرين.

.3.9أجهزة الحاسوب المحمولة والأجهزة الأخرى: لا يجوز تخزين البيانات السرية أو الحساسة على أجهزة الحاسوب المحمولة، أو أجهزة الايباد، أو أجهزة الكمبيوتر الدفترية، أو أجهزة الحاسوب الكفية، أو الأجهزة المماثلة، إلا إذا كانت محمية بعمليات تسجيل الدخول الموضحة أعلاه. يتحمل المستخدمون مسؤولية فردية عن الأمن المادي لهذه الأجهزة وسرية المعلومات والوثائق الموجودة عليها.

أجهزة [illegible] وسائط تخزين

عمليات الكتابة عن بعد: يجب وضع الضوابط اللازمة لمنع الوصول غير المصرح به إلى البيانات السرية أو الخاصة (البيانات المحددة في القسم 3.11) أثناء

يجب على المستخدمين التأكد من طباعة المعلومات السرية على طابعة آمنة أو أن عملية الطباعة تتم تحت إشراف شخص مخول يمكنه مراجعة المواد المطبوعة.

مشاركة ونقل البيانات السرية والخاصة: .3.12

لا يجوز للمستخدمين إنشاء اتصالات ذاكرة إلكترونية، أو شبكات محلية، أو خوادم نقل ملفات (FTP)، أو خوادم ويب، أو اتصالات مودم بشبكات محلية قائمة أو أنظمة متعددة المستخدمين أخرى لغرض نقل المعلومات دون إذن مسبق من قسم تقنية المعلومات. ويُسمح فقط للموظفين المصرح لهم تحديدًا من قبل مدير تقنية المعلومات، والذين يتمتعون بصلاحيات وصول خاصة، بإنشاء هذه الخدمات.

.3.13التخلص من المعدات وبيئات التخزين وإعادة تدويرها

الإزالة: إذا كان سيتم إرسال وسائط تخزين الكمبيوتر إلى مورد للاستبدال أو الصيانة أو الإتلاف، فسيتم إتلاف جميع البيانات السرية والخاصة أو إخفاؤها باستخدام الطرق المعتمدة.

تعليق وإلغاء امتيازات الوصول: .3.14

.3.14.1وصول المستخدم إلى أصول المعلومات التي يحتفظ بها مالكو أصول المعلومات

يتحمل مالك أصول البيانات مسؤولية وضع الإرشادات المطبقة لإلغاء الصلاحيات. ويتولى الموظفون المعينون من قبل مالك أصول البيانات تنفيذ عمليات منح وإلغاء حقوق الوصول للمستخدمين نيابةً عنه، وفقًا للإرشادات المحددة.

.3.14.2يتحمل رؤساء الأقسام مسؤولية الإبلاغ الفوري عن أي تغييرات في تعيينات المستخدمين أو حالتهم الوظيفية التي تتطلب تعديلات على صلاحيات الوصول الممنوحة لهم. في حالة إنهاء الخدمة، يتولى مدير الموارد البشرية إدارة عملية إلغاء حقوق وصول المستخدم المعني إلى جميع البيانات والمعلومات والأنظمة، وإخطار مدير تقنية المعلومات بذلك.

.3.14.3يتحمل رؤساء الأقسام مسؤولية مراجعة وتحديث نظام صلاحيات الوصول المخصصة للمستخدمين مرة واحدة سنويًا. وفي حال تغيير صلاحيات الوصول، يقوم رؤساء الأقسام بإجراء التعديلات التفصيلية اللازمة في آلية إدارة حسابات المستخدمين.

.3.14.4في حال إنهاء علاقة المستخدم مع كارديلين بويا، يقوم رئيس القسم المختص بمراجعة ملفات الحاسوب الداخلية والملفات الورقية المحفوظة يدويًا على الفور لتحديد المسؤول عن حفظها و/أو الطرق المناسبة لإتلافها. بعد ذلك، يُعيد رئيس القسم تحديد مهام مستخدم الحاسوب بتفويض مسؤولية الملفات التي كانت مُسندة إليه سابقًا إلى مستخدم جديد. .3.14.5تُعلق حسابات المستخدمين التي لم تُسجل أي نشاط لمدة ثلاثة أشهر تلقائيًا. ويُعيد رئيس القسم المختص تحديد صلاحيات الوصول للمستخدمين الذين يستأنفون مهامهم بعد إجازة أو مهمة مؤقتة أو إجازة غير مدفوعة الأجر تتجاوز شهرًا واحدًا.

.3.14.6الجلسة: إذا لم يُرصد أي نشاط على محطة العمل لمدة عشرين دقيقة، يجب على النظام خفض سطوع الشاشة تلقائيًا وإنهاء الجلسة. ولا يُسمح بإعادة الدخول إلى الجلسة إلا بعد إدخال المستخدم لكلمة المرور الصحيحة. .3.14.7إدارة كلمات المرور: يجب تشفير كلمات المرور وقوائم التحكم في الوصول ومعلومات التحكم في الوصول الأخرى عند تخزينها أو نقلها عبر الشبكة. ويجب وضع الضوابط اللازمة لمنع الوصول غير المصرح به إلى كلمات المرور المخزنة ومعلومات التحكم في الوصول واستخدامها. .3.14.8لا ينبغي تضمين كلمات المرور مباشرةً (برمجتها) في البرامج أو التطبيقات للسماح بتغييرها عند الضرورة.

.3.14.9يجب أن تكون كلمات المرور الممنوحة للمستخدمين الجدد صالحة فقط لتسجيل دخول المستخدم الأول. بعد تسجيل الدخول، يجب على المستخدم تعيين كلمة مرور جديدة. وينطبق الإجراء نفسه على إعادة تعيين كلمة المرور في حال نسيانها.

.3.14.10يجب تغيير كلمات المرور الافتراضية على الأجهزة المُستلمة من الموردين قبل استخدامها لأول مرة. ينطبق هذا الإجراء على بيانات اعتماد المستخدم النهائي، بالإضافة إلى بيانات اعتماد مسؤول النظام وغيره من المستخدمين ذوي الصلاحيات الخاصة.

.3.14.11لا يجوز للمستخدمين مشاركة كلمات مرور حساباتهم الشخصية مع أي شخص، بما في ذلك مشرفي الوحدات والزملاء. ولمشاركة الملفات والمعلومات، يجب على المستخدمين استخدام أدلة الشبكة المحلية المشتركة، أو البريد الإلكتروني، أو صفحات الإنترانت، أو محركات الأقراص المرنة -وهي آليات معتمدة ومسموح بها من قبل قسم تقنية المعلومات.

.3.14.12تطوير النظام: سيتم استخدام المعايير الموضحة أدناه لمنع الأفراد غير المصرح لهم من الوصول إلى البيانات التي تم إنشاؤها بواسطة الشركة ولتحسين سلامة التطبيقات.

فصل بيانات المؤسسة وأنظمة التطوير والاختبار: يجب فصل البيانات التي يتم إنشاؤها في نهاية المطاف بواسطة عمليات الأعمال المؤسسية عن بيئات التطوير والاختبار.
وهذا يضمن حماية أفضل لمعلومات الشركة.
لا يُسمح، من حيث المبدأ، للعاملين في بيئات التطوير والاختبار بالوصول إلى أنظمة الشركة. ويقتصر حق الوصول إلى بيانات الشركة على رؤساء الأقسام فقط. وبالمثل، يجب على جميع عمليات اختبار برامج الشركة معالجة البيانات المُنقّاة، واستبدال المعلومات والبيانات السرية والخاصة ببيانات مُزوّرة. أنظمة الشركة ومعلوماتها...

ينبغي استخدام عمليات التحكم في التغيير الرسمية والموثقة لتقييد التغييرات والموافقة عليها.

تطوير البرمجيات: قبل نشر البرامج للاستخدام المؤسسي، يجب على مطوري البرامج وغيرهم من الموظفين التقنيين إزالة جميع طرق الوصول الخاصة لضمان أن يكون الوصول ممكنًا فقط من خلال الوسائل العادية والآمنة.

لذا، يجب إزالة جميع برامج الاختراق الخفية وغيرها من الاختصارات التي قد تُستخدم لاختراق أمن النظام. كما يجب تحديد وتفعيل جميع إجراءات التحكم في الوصول على مستوى المستخدم ومستوى المسؤول، المنصوص عليها في سياسات ولوائح أمن المعلومات، قبل نشر الأنظمة المطورة للاستخدام المؤسسي.

ضوابط ترحيل البيئة: بعد اكتمال مراحل تطوير البرمجيات واختبارها، ينبغي تطبيق منهجية مناسبة لضمان تنفيذ عملية ترحيل البرمجيات إلى منصات المؤسسة بطريقة منظمة ومضبوطة. يجب ألا يتمتع موظفو تطوير التطبيقات بصلاحية الوصول المباشر لتحميل البرمجيات إلى بيئات تقنية المعلومات الخاصة بالمؤسسة. كما يجب وضع ضوابط ضرورية لمنع ترحيل أي شفرة برمجية غير مصرح بها إلى بيئة تقنية المعلومات الخاصة بالمؤسسة.

ينبغي أن تقتصر صلاحيات الوصول التي تُدخل تغييرات على عمليات إنتاج المعرفة المؤسسية على تطبيقات إنتاج المعرفة المؤسسية فقط. عند تحديد الصلاحيات، لا ينبغي السماح لمستخدمي النظام بتعديل بيانات النظام دون قيود. يجب على المستخدمين استخدام بيانات المؤسسة لتعزيز وحماية سلامة الأنظمة.

ينبغي أن يكون بإمكانهم فقط إجراء تغييرات على التنسيقات المحددة مسبقًا.
يجب إجراء تحديثات قواعد بيانات الشركة باستخدام طرق محددة معتمدة من الإدارة العليا. ولا يُسمح باستخدام أدوات الوصول المباشر إلى قواعد البيانات في بيئة إنتاج المعلومات بالشركة، لأن هذه البرامج قد تُخالف إجراءات مزامنة قواعد البيانات ونسخها، وروتينات معالجة أخطاء الإدخال، وآليات التحكم الأخرى الهامة.

السجلات وأدوات الأمان الأخرى: يجب على أنظمة الحاسوب والاتصالات التي تحتوي على بيانات سرية أو حساسة تسجيل جميع الأحداث الأمنية الهامة. ومن أمثلة هذه الأحداث: تغيير المستخدمين لبيانات اعتمادهم أثناء الجلسات عبر الإنترنت، ومحاولات تخمين كلمات المرور، ومحاولات استخدام صلاحيات وصول غير مصرح بها، والتعديلات على برامج تطبيقات الشركة، والتغييرات التي تطرأ على برامج النظام والتي تُغير صلاحيات المستخدم، والتعديلات على أنظمة التسجيل الفرعية.

سيقوم مدير تكنولوجيا المعلومات بتقديم تقارير دورية إلى الإدارة العليا حول التطورات والأحداث والمواقف ومستويات الامتثال للسياسات والتغييرات وغيرها من الأمور المتعلقة بأمن الوصول.

متطلبات الإبلاغ: يجب الإبلاغ فوراً إلى أقرب مشرف وحدة أو فريق الدعم الفني لتكنولوجيا المعلومات عن أي وصول غير مصرح به أو محاولة وصول، أو سرقة أو إفشاء كلمات المرور أو ضوابط الوصول، أو الاشتباه في فقدان البيانات أو تغييرها أو إفشائها، أو انتهاكات معايير أو إجراءات أو سياسات الأمان، وذلك عن طريق تعبئة النموذج المرفق بخطة الاستجابة لخرق البيانات.

.4التحكم في الوصول المادي: نظرًا لحساسية الموارد والبيانات الموجودة داخل المرافق التي تستخدمها شركة ،Kardelen Boyaففي حالة وجود قيود على الوصول، سيتم تنفيذ التحكم في الوصول بشكل أساسي بواسطة Kardelen Boyaباستخدام تقنية .RFID

سيتم توفير ذلك عبر بطاقات الهوية. بيانات غرفة النظام وبيانات البحث والتطوير.

يجوز استخدام أنظمة التعرف على بصمات الأصابع للدخول إلى المنطقة، شريطة الحصول على إذن كتابي مسبق من المدير العام. ولا يجوز استخدام أنظمة التعرف على البطاقات وبصمات الأصابع إلا للسماح بالدخول إلى المناطق المخصصة للموظفين المصرح لهم فقط، ويُحظر استخدامها مطلقًا لمراقبة التزام الموظفين بساعات العمل.

.4.1في حالة فقدان بطاقات هوية ،Kardelen Boyaيجب الإبلاغ عن الوضع إلى قسم تكنولوجيا المعلومات على الفور.

يتم إخطار الشخص المسؤول. ويتأكد مدير تقنية المعلومات فورًا من حذف البطاقة المعنية من نظام التحكم في الوصول المادي للشركة. ولن تُصدر بطاقة بديلة إلا بعد إلغاء البطاقة المفقودة. وستتمتع البطاقة البديلة بنفس صلاحيات الوصول التي كانت تتمتع بها البطاقة القديمة.

.4.2البيانات التي يجب الاحتفاظ بها في أنظمة التحكم في الوصول: تشمل البيانات التي تحتفظ بها الشركة فيما يتعلق بنظام التحكم في الوصول ما يلي:

•بيانات حامل البطاقة: oالاسم واللقب

المسمى الوظيفي، القسم، عنوان البريد الإلكتروني، رقم تسجيل الموظف، رقم الهاتف المحمول

•البطاقات المخصصة لحامل البطاقة

•موقع وتاريخ ووقت عملية قراءة البطاقة

.4.2.1يجوز للموظفين الذين تتطلب مهامهم الوصول إلى برامج التحكم في الوصول الوصول إلى بيانات التحكم في الوصول. ويشمل هؤلاء الموظفون ما يلي:

•حراس الأمن •الفنيون الذين يصدرون بطاقات الدخول أو يقومون بإجراءات استبدال البطاقات وإتلافها

•موظفو الدعم الفني لتكنولوجيا المعلومات .4.2.2في الحالات التي يتم فيها نقل البيانات من نظام التحكم في الوصول إلى المستلم الطالب،

وفقًا للإجراءات الموضحة في هذه السياسة، يجب، حيثما أمكن عمليًا، إزالة جميع الحقول التي تُتيح تحديد هوية البيانات على أنها تخص شخصًا معينًا. على سبيل المثال، إذا رغبنا في معرفة عدد الأشخاص الذين استخدموا قارئًا خلال فترة زمنية محددة، فلن يكون من الضروري الكشف عن أسماء حاملي البطاقات أو صورهم أو أي معلومات شخصية أخرى في التقرير؛ بل سيتم إرسال البيانات المتعلقة بعملية قراءة البطاقة فقط.

.4.3أساليب التحكم في الوصول

يتم توفير الوصول إلى البيانات بطرق مختلفة باستخدام الأساليب المذكورة أدناه، وفقًا لمستويات تصنيف البيانات.

تتضمن طرق التحكم في الوصول المستخدمة افتراضيًا ما يلي:

•افتح تسجيل الدخول على الأجهزة،

•مشاركة الملفات وأذونات الملفات والمجلدات في نظام ويندوز،

•قيود امتيازات حساب المستخدم،

•حقوق الوصول إلى الخادم ومحطة العمل،
•أذونات جدار الحماية،
•قوائم التحكم في الوصول إلى مناطق الشبكة وشبكات VLAN،
•حقوق المصادقة على الشبكة الداخلية/الخارجية،
•حقوق تسجيل دخول المستخدم Kardelen Boya،
•حقوق الوصول إلى قواعد البيانات وقوائم التحكم في الوصول،
•التشفير أثناء التخزين وأثناء التنقل.
•طرق أخرى يشترطها العقد من قبل الأطراف المعنية

4.4.ينطبق التحكم في الوصول على جميع الشبكات والخوادم ومحطات العمل المملوكة لشركة Kardelen Boya. ينطبق هذا على أجهزة الكمبيوتر المحمولة والأجهزة المحمولة.

4.5.سيتم استخدام التحكم في الوصول القائم على الأدوار كطريقة لتأمين الوصول إلى جميع الموارد القائمة على الملفات الموجودة في مجالات Active Directory الخاصة بـ Kardelen Boya.

4.6.اختبار الاختراق: سيخضع نظام التحكم في الوصول الخاص بشركة كارديلين بويا لاختبارات اختراق دورية لتحديد مدى فعالية الضوابط الحالية والكشف عن أي نقاط ضعف. وعند الاقتضاء والاتفاق، ستشمل هذه الاختبارات أيضًا أنظمة مزودي خدمات الحوسبة السحابية.

للاستفسارات المتعلقة ببيانات التحكم في الوصول
مخطط سير العملية الحالي