سياسة تنظيم أمن المعلومات **(ISR)**

Version 1.0

تسري التعاريف الموجودة في هذا القسم 2 على سياسة تنظيم أمن المعلومات (ISR) هذه بأكملها.

التعاريف	التفسيرات
الإتفاقية	الإتفاقية بين فلاي دبي وطرف ثالث والتي سيحصل الطرف الثالث بموجبها على بيانات فلاي دب
الأطراف المصرّح لها	كلّ الموظّفين لدى الطرف الثالث، إضافة إلى وكلائه وممثليه وأي طرف آخر يكون اشتراكه ووصوله إلى بيانات فلاي دبي ضرورياً قطعاً، في جميع الحالات، لأداء التزامات الطرف الثالث المنصوص عليها في الإتفاقية.
خطة التصدي للأزمات وضمان استمرارية الأعمال	مجموعة عمليّات وتقنيّات تُستخدم لمساعدة منظّمة على التعافي من كارثة ومواصلة أو استئناف العمليات التجارية الروتينية.
المعلومات السريّة	معلومات تمّ الكشف عنها من قِبل (أو بالنيابة عن) طرف أو ممثّليه لصالح الطرف الآخر في ما يتعلّق بالإتفاقية، وتكون هذه المعلومات مصحوبة بعلامة تميّزها على أنّها سرية أو تُعتبر سرية بالمنطق في ظلّ الظروف الراهنة.
بروتوكول التهيئة الآليّة للمُضيف	بروتوكول إدارة شبكة يُستخدم على شبكات بروتوكول الإنترنت لتعيين عناوين بروتوكول الإنترنت IP وباراميترات تواصل أخرى تلقائياً لأجهزة متّصلة بالشبكة باستخدام بنية عميل-خادم.
فلاي دبي	مؤسسة دبي للطيران (المتداولة تحت اسم 'فلاي دبي')
بيانات فلاي دبي	كلّ المعلومات التي تتعلّق بفلاي دبي أو أنشطتها التجارية أو عملائها بمختلف أشكالها، والتي تقدّمها فلاي دبي في ما يتعلّق بتأدية التزامات الطرف الثالث المنصوص عليها في الإتفاقية، وتشمل أي معلومات يتمّ تقديمها أو إصدارها أو جمعها أو معالجتها أو تخزينها أو نقلها في ما يتعلّق بوصولهم إلى و/أو باستخدامهم لالتزامات الطرف الثالث المنصوص عليها في الإتفاقية.
عمليّة إدارة الحوادث	مجموعة إجراءات وخطط عمل يجري تطبيقها للاستجابة إلى حوادث خطيرة وإيجاد حلول لها: طريقة اكتشاف الحادثة والإبلاغ عنها، وتحديد المسؤول عنها و الوسائل المستخدَمة والخطوات المتّخذة لإيجاد حلّ للحادثة.
الهواتف المحمولة والأجهزة المحمولة الأخرى	شكل صغير من أجهزة الحوسبة، مصّمم ليُحمل ويُستخدَم بواسطة اليد وليتّصل بشبكة الإنترنت وليتواصل مع أجهزة أخرى مشابهة له.
معلومات شخصية	معلومات أو رأي عن فرد معروف الهوية، أو عن فرد قد تعرف هويته بشكل معقول، بغضّ النظر عن صحّة المعلومات أو الرأي، وعن تسجيل المعلومات أو الرأي بشكل مادي، وتشمل على سبيل المثال لا الحصر البيانات الشخصية لأغراض النظام الأوروبي العام لحماية البيانات 2016/ 679.
السياسة	سياسة تنظيم أمن المعلومات هذه
الرخص التقييدية أو المتبادلة أو الموروثة أو المتروكة	تراخيص برمجيات تتطلّب أن تكون المعلومات الضرورية لاستنساخ وتعديل البرمجيات المماثلة متاحة للاطلاع العام لمتلقي الصيغ القابلة للتنفيذ من البرمجيات المماثلة بما فيها على سبيل المثال لا الحصر الرخصة العمومية الشاملة (GPL) ورخصة أفيرو العمومية الشاملة (AGPL) .
بوابة الأمن	مجموعة من آليات التحكم بين شبكتين أو أكثر تملك كلّ منها مستوى ثقة مختلف، بغرض تصفية كلّ المعلومات التي تمرّ أو تحاول أن تمرّ بين الشبكات، والخوادم الإدارية والتنظيمية المرتبطة بها، وتسجيلها.
آلية تحقق قوية	طريقة للتحقق من المستخدِم تعتبر قوية بما يكفي للصمود في وجه أي هجوم على النظام الذي ينفّذ المستخدمون عملية التحقق من خلاله.
تشفير قوي	استخدام تقنيات التشفير تستعمل مفتاح يتجاوز طوله 128 بت للتشفير المتماثل و1024 بت للتشفير غير المتماثل، بحيث تقدم قوتها ضمانات معقولة

	على أنّها ستحمي المعلومات المشفرة من الوصول غير المصرح له إليها وهي مناسبة لحماية سرية وخصوصية المعلومات المشفرة، كما أنّها تشمل سياسة موثّقة لتنظيم مفاتيح التشفير والعمليات المرتبطة بها، وهي مناسبة لحماية سرية وخصوصية المفاتيح وكلمات المرور المستخدَمة كمدخلات لخوارزمية التشفير.
تدابير أمن تنظيمية وتقنية	الوظائف، والعمليات، والضوابط، والأنظمة، والإجراءات والتدابير التي يمكن للمنظمات تطبيقها لضمان معالجة البيانات الشخصية والسرية وتخزينها بشكل آمن، ولتجنّب خرق البيانات، ولتسهيل الامتثال للالتزامات بحماية البيانات ذات الصلة.
الطرف الثالث	الطرف الثالث الذي يحظى بإمكانية الوصول إلى بيانات فلاي دبي المتعلّقة بهذه السياسة.

1. تنظيم أمن المعلومات

يجب على الطرف الثالث، كحدّ أدنى:

.أ. أن يضمن منح الأطراف المصرّح لها فقط إمكانية الوصول إلى بيانات فلاي دبي

ب. أن يطبّق تدابير أمن تنظيمية وتقنية لا تقلّ قوةً عن أفضل ممارسات أمن المعلومات لحماية سلامة بيانات فلاي دبي والمعلومات غير العامة الأخرى وتوافرها وسريّتها، ومنع الوصول غير المصرح به إلى بيانات فلاي دبي والاستحواذ عليها أو نشرها أو تدميرها أو .تعديلها أو فقدانها بشكل غير متعمّد أو سوء استخدامها أو إتلافها

ج. أن يضع أفضل الممارسات والسياسات ويطبّقها ويحافظ عليها، إلى جانب برنامج من تدابير الأمن التنظيمية والتقنية التنظيمية والتشغيلية والإدارية والمادية مع الحفاظ على توافقها مع أفضل ممارسات في هذا المجال، وذلك بغرض أن تكون مناسبة لـ (1) منع وصول أي من الأطراف غير المصرّح لها إلى بيانات فلاي دبي بأسلوب غير مصرّح به من خلال هذه الإتّفاقية وهذه السياسة، و (2) .الامتثال للقوانين والأنظمة المطبّقة والمعايير الصناعية المطبّقة وتلبيتها

د. أن يتّخذ خطوات معقولة لمنع الوصول غير المصرّح به إلى بيانات فلاي دبي والتزامات الطرف الثالث المنصوص عليها في الإتفاقية، .أو الأنظمة، أو الأجهزة، أو الوسائط التي تحتوي على هذه المعلومات، أو خسارة هذه البيانات

هـ. أن يستخدم عمليات وإجراءات تقييم المخاطر لتقييم الأنظمة المستخدَمة بشكل دوري، بغرض إتمام التزامات أو تقديم منتجات الطرف الثالث إلى فلاي دبي. سيكون على الطرف الثالث معالجة المخاطر المماثلة بأسرع ما يمكن ومطابقتها مع نسبة الخطر الذي تطرحه التهديدات المعينة على فلاي دبي والمعروفة عند اكتشافها. على الطرف الثالث وضع عمليّة ليتمكن من إبلاغ فريق الأمن لدى .فلاي دبي بالمخاطر أو الحوادث المحتملة

و. أن يحتفظ بسجلات عن الأطراف المصرّح لها ومصادر معلومات الطرف الثالث التي يمكنها الوصول إلى بيانات فلاي دبي أو تحويلها .أو الاحتفاظ بها أو تخزينها أو معالجتها

ز. إجراء تحريات شاملة عن جميع الأطراف المصرح لها قبل توظيفهم بقدر ما يجيزه القانون. يجب أن تشمل التحريات الشاملة عن الأفراد، كحد أدنى، سيرة الفرد المهنية السابقة، وسجله الجنائي، وسجلاته الائتمانية، إلى جانب التحقق من جهاته المرجعية، .والتحريات الإضافية التي تقتضيها المتطلبات التجارية الإضافية

ح. أن يفرض على الأطراف المصرّح لها توقيع التزامات تعاقدية بعدم الكشف عن المعلومات والسرية قبل إعطائهم إمكانية الوصول إلى .بيانات فلاي دبي

ح. أن يتأكّد من أنّ جميع الأطراف المصرح لها التي قد تقوم بأعمال منصوص عليها في الإتفاقية أو قد تحظى بإمكانية الوصول إلى بيانات فلاي دبي تمتثل لتدابير الأمن التنظيمية والتقنية هذه، على أن تشهد على ذلك اتفاقية خطية لا تقلّ تقييداً عن هذه السياسة.

2. الأمن المادي والبيئي

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يتأكّد من أنّ جميع أنظمة الطرف الثالث ومصادره الأخرى التي وضعت بغرض أن يستخدمها العديد من المستخدمين مخزنة في .مرافق مادية آمنة تتمتع بإمكانية وصول محدودة وتقتصر على الأفراد المصرّح لهم فقط

ب. أن يراقب ويسجّل الوصول إلى المرافق المادية التي تحتوي على الأنظمة والمصادر الأخرى التي وضعت بغرض أن يستخدمها العديد من المستخدِمين لغرض إعادة التدقيق فيها، والتي تستخدم في ما يتعلّق بتأدية التزامات الطرف الثالث المنصوص عليها في الإتفاقية.

ج. أن يراقب إمكانية وصول الأشخاص إلى مرافقه ويحدّها بالأطراف المصرّح لها فقط

د. أن يحافظ عن طريق أشخاص، على أمن المعدات المستخدَمة لتخزين بيانات فلاي دبي أو معالجتها أو نقلها، بما في ذلك نقاط الوصول اللاسلكية، والبوابات الإلكترونية، والأجهزة المحمولة يدوياً، ومعدّات الربط الشبكي والتواصل، وخطوط الاتصالات السلكية واللاسلكية.

هـ. أن يطبّق ضوابط للحدّ من خطر التهديدات المادية والحماية منها.

و. أن يحمي أي جهاز يسجّل بيانات بطاقة الدفع بواسطة التفاعل الجسدي المباشر من العبث بها أو تبديلها عن طريق التحقق دورياً من سطح الأجهزة لكشف العبث أو التبديل؛ وأن يدرّب الطاقم ليلاحظ محاولات العبث بالأجهزة أو تبديلها.

3. التحكم بالوصول

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يفصل بين بيانات فلاي دبي وبيانات عملاء الطرف الثالث الآخرين أو بينها وبين تطبيقات فلاي دبي الخاصة ومعلوماته سواء كان ذلك باستخدام خوادم منفصلة أو باستخدام آليات التحكم بالوصول المنطقية التي لا تتطلّب الفصل المادي بين الخوادم.

ب. أن يتعرف إلى المالكين وأن يطلب منهم مراجعة حقّ الوصول إلى الأنظمة المستخدَمة للدخول إلى بيانات فلاي دبي أو معالجتها أو تنظيمها أو تخزينها، والموافقة على ذلك، بشكل فصلي على الأقل لمنع أشكال الوصول غير المصرّح بها؛ وأن يحافظ على عملية الموافقة على الوصول ويتعقبها.

ج. أن يوقف الوصول إلى الأنظمة التي تنظّم بيانات فلاي دبي في غضون 24 ساعة من فسخ علاقة الطرف المرخص له مع الطرف الثالث؛ وأن يطبّق إجراءات معقولة لإنهاء وصول الأطراف إلى هذه الأنظمة خلال ثلاثة أيام عمل عندما تسقط الحاجة إليها وتنعدم أهميّتها لأداء واجباتها. يجب تعليق العمل بهويات المستخدمين الأخرى كلها أو إزالتها بعد 90 يوماً تقويمياً من التوقف عن العمل.

د. أن يحدّ من إمكانية وصول مدير النظام (المعروف أيضاً بالمستخدم الأساسي، صاحب الامتيازات أو المستخدم الخارق) إلى الأنظمة التشغيلية المخصّصة للاستخدام من قبل العديد من المستخدمين بالأفراد الذين يحتاجون إلى إمكانية وصول مماثلة لأداء عملهم. كما أن يستخدم نظام التدقيق بهويات مدير النظام بواسطة بيانات دخول فردية خاصة وسجلات أنشطة لتنظيم الوصول الخاضع لحماية أمنية مشدّدة وحصر الوصول رفيع المستوى بعدد محدود للغاية من المستخدمين. أن يفرض على التطبيقات وقواعد البيانات والشبكات ومدراء النظام الحد من وصول المستخدمين إلى الأوامر والبيانات والأنظمة والمصادر الضرورية الأخرى لتنفيذ الوظائف المصرّح لهم بها. يجب مراجعة أدوار مدراء النظام ولوائح الوصول أقله مرة سنوياً.

هـ. أن يفرض آلية تحقق قوية على جميع أنواع الوصول الإداري اللاسلكي، أو أي وصول عن بُعد وجميع أنواع الوصول الإداري إلى بيئة الشبكة السحابية.

4. التعرّف والتحقّق

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يصدرهوية مستخدم فريدة لكل مستخدم وأن يزود كلّ حساب بآلية تحقّق خاصة.

ب. أن يستخدم عملية تنظيم موثّقة لدورة حياة هوية المستخدم تشمل، على سبيل المثال لا الحصر، الإجراءات المطلوبة لإنشاء حساب موافق عليه، وإزالة الحسابات في الوقت الملائم، وتعديل الحسابات (مثلاً تغيير الامتيازات، ومدى إمكانية الوصول، والوظائف/ الأدوار) الخاصة بجميع أشكال الوصول إلى بيانات فلاي دبي وفي جميع البيئات (مثلاً الإنتاج، والاختبار، والتطوير، وما إلى ذلك...). يجب أن تشمل الإجراءات المماثلة مراجعة امتيازات الوصول والتحقق من صلاحية الحسابات أقلّه فصلياً.

ج. أن يحصر كل أشكال الوصول إلى بيانات فلاي دبي بالأفراد الذين يستخدمون هوية مستخدم وكلمة مرور صالحتَين، وأن يفرض على مستخدمي الهويات الفريدة اعتماد أحد هذه الخيارات: كلمة مرور أو جملة مرور، أو آلية تحقق من خطوتين، أو التحقّق البيومتري.

د. أن يفرض استخدام كلمة مرور معقّدة تستوفي شروط إنشاء كلمة مرور التالية المنصوص عليها في سياسة فلاي دبي: استخدام ثمانية (8) رموز أقلّه لكلمات المرور الخاصة بالنظام، وأربعة (4) رموز أقلّه لكلمات المرور الخاصة بالأجهزة اللوحية والهواتف الذكية. يجب أن تحتوي كلمات المرور الخاصة بالنظام على أحرف وأرقام ورموز خاصة.

هـ. لا يجب أن تكون كلمة المرور مماثلة لهوية المستخدم الخاصة بها، ولا يجب أن تحتوي على كلمة يمكن إيجادها في المعجم، أو على أرقام متتالية أو متكرّرة، ولا يجب أن تكون هي نفسها إحدى كلمات المرور الخمس التي تم استخدامها سابقاً.

و. أن يفرض تاريخ لانتهاء صلاحية كلمة المرور بشكل دوري وبفترة لا تتخطّى تسعين (90) يوماً.

ز. أن يخفي كلمات المرور أثناء عرضها.

ح. أن يضع حد لمحاولات الدخول الفاشلة بخمس (5) محاولات دخول فاشلة خلال 24 ساعة ويغلق حساب المستخدم عند الوصول إلى هذا الحدّ بشكل متكرر. يمكن إعادة تنشيط الحساب بعد ذلك من خلال عملية يدوية تتطلب التحقق من هوية المستخدم.

ط. أن يتحقّق من هوية المستخدم ويحدّد شروط الاستخدام لمرة واحدة وشروط إعادة ضبط كلمات المرور برمز فريد لكل مستخدم. وأن يحث المستخدم تلقائياً على تغيير كلمة المرور بعد الاستخدام الأول.

ي. أن يستخدم طريقة آمنة لإرسال بيانات الاعتماد الخاصّة بالتحقّق (مثلاً كلمات المرور) وآليات التحقّق (مثلاً الرموز أو البطاقات الذكيّة).

ك. أن يضع حدًّا أدنى من 12 رمزاً لعدد الرموز التي تتألّف منها كلمات المرور الخاصّة بحسابات الخدمة وحسابات الوكيل، على أن تشمل أحرفاً كبيرة وصغيرة وأرقاماً ورموزاً خاصّة. يجب تغيير كلمات مرور حسابات الخدمة وحسابات الوكيل أقلّه مرّة في العام وبعد فسخ عقد التوظيف مع أحد الأفراد الذين يعرفون كلمة المرور.

ل. أن ينهي الجلسات التفاعليّة أو يفعّل شاشة قفل آمنة تتطلّب آليّة تحقّق بعد فترة توقف عن العمل لا تتخطّى خمس عشرة (15) دقيقة.

م. أن يستخدم طريقة تحقّق تأخذ بالاعتبار حساسيّة بيانات فلاي دبي. يجب على الطرف الثالث أن يحمي بيانات الاعتماد الخاصّة بآليّة التحقّق باستخدام التشفير القوي كلما جرى تخزين هذه البيانات.

ن. أن يضبط النظام ليقفل تلقائياً بعد فترة توقّف لا تتجاوز: 15 دقيقة للخادم، 15 دقيقة لمحطة العمل، 4 ساعات للهاتف المحمول، 7 أيام لبروتوكول التهيئة الآلية للمُضيف، و24 ساعة للشبكة الافتراضيّة الخاصّة.

5 .الاستحواذ على أنظمة المعلومات، وتطويرها وصيانتها

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يستخدم منهجيّة فعّالة لإدارة التطبيق الذي يُدخل تدابير الأمن التنظيمية والتقنية في آلية تطوير البرمجيّات، وأن يتأكّد من أنّ .الطرف الثالث يطبّق تدابير الأمن التنظيميّة والتقنيّة بانتظام، وفقاً لأفضل الممارسات في هذا المجال

ب. أن يتّبع إجراءات تطوير تستوفي المعايير الصناعيّة، وتشمل الفصل بين الشيفرات الخاصّة بالبيئات المنتجة وتلك الخاصّة بالبيئات .غير المنتجة في ما يتعلّق بأساليب الوصول وكلمات المرور، وفصل المهام المرتبطة بها بين البيئات المماثلة

ج. أن يتأكّد من تقييم الضوابط الداخليّة لأمن المعلومات الخاصّة بتطوير البرمجيّات بانتظام، بشكل يعكس أفضل الممارسات في هذا .المجال، وأن يعيد النظر في هذه الضوابط ويطبّقها بشكل دوري

د. أن يتحكّم بأمن عملية التطوير وأن يتأكّد من الالتزام بممارسات تشفير آمنة وتطبيقها، بما في ذلك كتابة الشيفرات بأسلوب ملائم، .والحماية من الشيفرات الخبيثة، ومراجعة الشيفرات المكتوبة على يد زملاء المهنة

هـ. أن يجري اختبارات ضد الاختراق على التطبيقات المنجَزة بالكامل قبل بدء إنتاجها وبعد ذلك، أقّله مرّة سنوياً وبعد تطبيق أي ، ومعايير فريق (OWASP) تعديل ملحوظ على الشيفرة الأصليّة أو بعد إعادة الضبط بما يتّفق مع مشروع أمان تطبيق الويب المفتوح ، وتقرير معهد إدارة النظم والمراجعة والشبكات والأمن الذي يشمل أبرز 25 نقطة ضعف (CERT) الاستجابة للطوارئ المجتمعية كذلك عليه إجراء كلّ الإصلاحات .(PCI-DSS) ، ومعايير حماية بيانات البطاقات الائتمانيّة المصرفيّة(SANS Top 25) شائعة .للثغرات القابلة للاستغلال قبل إعادة التطبيق إلى مرحلة الإنتاج

و. أن يستخدم البيانات مجهولة المصدر أو محجوبة المصدر في البيئات غير المنتجة. وألّا يستخدم أبداً بيانات إنتاج نص عادي في أي بيئة غير منتجة، وألّا يستخدم المعلومات الشخصيّة في البيئات غير المنتجة لأي سببٍ من الأسباب. كذلك، أن يتأكّد من حذف .بيانات وحسابات الاختبار قبل بدء الإنتاج

ز. أن يعيد النظر في الشيفرات مفتوحة المصدر أو حرّة المصدر الموافق عليها من قبل فلاي دبي، أو البرمجيات أو التطبيقات أو الخدمات بغرض البحث عن أي عيوب أو أخطاء أو مشاكل تتعلّق بالأمن أو عدم امتثال لأحكام الرخص الخاصّة بالمصادر المفتوحة أو الحرّة. يجب على الطرف الثالث إبلاغ فلاي دبي مسبقاً عن استخدام شيفرات من مصادر مفتوحة أو حرّة، وإذا وافقت فلاي دبي على هذا الاستخدام، على الطرف الثالث تزويدها بإسم المصدر المفتوح أو الحرّ وبنسخته وعنوانه الإلكتروني. سيعترف الطرف الثالث ويقرّ بأنّ

(i) أي مصدر مفتوح أو حرّ يستخدمه في منتجاته أو خدماته يجب أن يحمل رخصة شيفرة "متساهلة" مفتوحة أو حرّة المصدر، وليس رخصة تقييديّة أو متبادلة أو موروثة أو متروكة؛

(ii) الطرف الثالث يحتفظ بحق تنقيح الشيفرات مفتوحة أو حرّة المصدر وتعديلها، ودمج الشيفرات مفتوحة أو حرّة المصدر أو الشيفرات التي تحتوي على مصادر مفتوحة أو حرّة مع شيفرة الملكيّة المسجّلة بدون وضع قيود على هذه التعديلات أو التنقيحات أو هذا الدمج مع شيفرة الملكيّة المسجّلة الذي يشتمل على شيفرات مفتوحة أو حرّة المصدر، وكيفية ترخيصها بعد ذلك (يُشار إليها الأعمال المشتقّة التالية لن تخضع لأي رخصة مصدر مفتوح أو حر تتطلّب ترخيص (iii)مجتمعةً بمصطلح "الأعمال المشتقّة") و .العمل المشتق أو جعله متوفراً بدون أي كلفة إضافيّة لأطراف ثالثة بحسب أحكام الرخصة مفتوحة أو حرّة المصدر

ح. ألّا يشارك أي شيفرة مستحدثة بحسب ما تنصّ عليه الإتفاقيّة، بغض النظر عن مرحلة تطويرها، في أي بيئة متشاركة أو غير خاصّة، .مثل مستودع شيفرات مفتوح، بغضّ النظر عن نسبة أمان كلمة المرور

6 .سلامة البرمجيّات والبيانات

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يمتلك، في بيئات تتوفر فيها البرمجيات المضادة للفيروسات تجارياً، برنامجاً مضاداً للفيروسات محدّثاً ومثبّتاً ومشغّلاً يمسحها للتأكّد من عدم وجود فيروسات وبرمجيّات خبيثة في أي نظام أو جهاز منها أو إزالتها منها أو عزلها تلقائياً.

ب. أن يفصل ما بين المعلومات والمصادر غير المنتجة وبين المصادر والمعلومات المنتجة.

ج. أن يتأكّد من أنّ فرق العمل تستخدم آليّة موثّقة للتحكّم في تغييرات النظام، ما يشمل إجراءات الانسحاب الخاصة بجميع البيئات المنتجة وآليّات التعامل مع التغيرات المفاجئة. وأن يضمّ الاختبار والتوثيق والموافقات على جميع التغيّرات التي قد يحدثها على النظام وأن يطلب موافقة إداريّة لإحداث تغييرات ملحوظة في الآليّات المماثلة.

د. أن يبني لائحة معايير أمان متعلقة ببيانات بطاقة الدفع ويحافظ عليها في حال كان الطرف الثالث يعالج بيانات حاملي البطاقات أو يخزّنها.

هـ. أن يفعّل خاصية تسجيل المعاملات المدقق بها في قاعدة بيانات خاصة بالتطبيقات التي تستخدم قاعدة بيانات تسمح بوضع تعديلات على بيانات فلاي دبي وأن يديرها، كما أن يحتفظ بسجلات عن المعاملات المدقّق بها لمدّة عام واحد (1) على الأقل فيما يبقيها لثلاثة أشهر متوفّرةً للمعالجة الفورية.

و. أن يعيد النظر في البرمجيّات ليجد الثغرات الأمنية ويعالجها خلال مرحلة التطبيق الأولي وعند بروز أي تغيّرات أو تطبيق تحديثات ملحوظة.

ز. أن يقوم بالتحقّق من جودة عناصر نظام الأمن (مثلاً، اختبار خاصيّة التعرّف، وخصائص التحقق والتصريح)، إضافةً إلى أي أنشطة أخرى مخصّصة للتحقق من بنية نظام الأمن، وذلك خلال مرحلة التطبيق الأولي وعند بروز أي تغيّرات أو تحديثات ملحوظة.

7 .أمن النظام

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن ينشئ أحدث الإصدارات الخاصّة بتدفّق البيانات ومخطّطات النظام المستخدمة للوصول إلى بيانات فلاي دبي أو معالجتها أو إدارتها أو تخزينها، وأن يحدّث هذه الإصدارات بانتظام.

ب. أن يراقب موارده الصناعيّة باستمرار (مثلاً موقع www.cert.org والقوائم والمواقع الإلكترونيّة الخاصّة بمورّدي البرمجيّات) للتبليغ عن جميع الإنذارات الأمنيّة المتعلّقة بأنظمة الطرف الثالث وموارد المعلومات الأخرى في الوقت المناسب (المتعلقة بها.

ج. أن يدير مفاتيح التشفير بأسلوب فعال عبر حدّ الوصول إلى هذه المفاتيح إلى أقلّ عدد ممكن من القيّمين، وتخزين مفاتيح التشفير السريّة والخاصّة باستخدام آليّة تحقّق تشمل مفتاحاً يوازي بقوتّه مفتاح التحقّق الذي يحمي البيانات على الأقّل، وأن يخزّنها في جهاز تشفير آمن منفصل عن مفتاح التحقّق الذي يحمي البيانات، وفي أقّل عدد ممكن من المواقع. كما عليه أن يغيّر مفتاح التشفير من الحالة المبدئية عند التنزيل وأقّله مرّتَين في العام، وأن يتخلّص من المفاتيح القديمة بشكل آمن.

د. أن يمسح الأنظمة الخارجية والداخلية وموارد المعلومات الأخرى والتي تشمل، على سبيل الذكر لا الحصر، الشبكات، والخوادم، والتطبيقات وقواعد البيانات، التي تضم برمجيّات ماسحة للثغرات الأمنية القياسية المطبقة في هذا المجال لاكتشاف الثغرات الأمنيّة، وضمان تحصين الأنظمة المماثلة والموارد الأخرى بالشكل الملائم، والتعرّف إلى أي شبكات لاسلكية غير مصرّح بها أقلّه بشكل فصليّ، وقبل إطلاق التطبيقات، وعند إدخال تغييرات ملحوظة إليها أو تحديثات في المهل الزمنية المحدّدة بحسب تحليلات المخاطر المرتكزة على السياسات والمعايير المتعلّقة بتكنولوجيا المعلومات والتي تكون معقولة ومقبولة في العموم.

هـ. أن يتأكّد من تحصين جميع أنظمة الطرف الثالث وموارده الأخرى ومن بقائها على هذا الحال بواسطة ممارسات تشمل، على سبيل مثلاً خدمات ومنتجات بصمة) المثال لا الحصر، إزالة الشبكات والخدمات والمنتجات الأخرى غير المستخدمة أو تعليق العمل بها وإقامة جدار حماية، ومضمّنات بروتوكول رصد ((TCP/IP) ، ونظام بروتوكول رصد الإرسال/ بروتوكول الإنترنتftp، وrloginاليد، و أو تكنولوجيا مماثلة (TCP) الإرسال.

أو أنظمة كشف ومنع التسلل (IPS) ، أو أنظمة منع التسلّل(IDS) و. أن يستخدم واحداً أو أكثر من هذه الأنظمة: أنظمة كشف التسلّل في أسلوب تشغيل نشط يراقب كلّ المعلومات الواردة إلى الأنظمة وتلك الخارجة منها فضلاً عن الموارد الأخرى بالتزامن مع (IDP) الاتفاقيّة في البيئات حيث تتوفّر هذه التكنولوجيا تجارياً وإلى أقصى حد ممكن عملياً.

ز. أن يفعّل آليّة تقييم المخاطر لاكتشاف الثغرات وتقييمها بالتماشي مع أفضل الممارسات في هذا المجال، لإصلاح الثغرات الأمنية في أي نظام أو في أي مورد آخر، ويشمل ذلك على سبيل المثال لا الحصر، الثغرات المُكتشَفة في المنشورات الخاصّة بالقطاع، والمسح لاكتشاف الثغرات والفيروسات، ومراجعة سجلّات الأمن، وتطبيق ملفات التصحيح الأمنيّة المناسبة على الفور، إذ من المحتمل أن يتم استغلال هذه الثغرات للولوج إلى النظام حالياً أو في المستقبل. يجب إصلاح الثغرات الخطرة المكتشَفة خلال التقييم وينبغي تطبيق ملفات التصحيح عليها على الفور عند توفّرها وفي فترة لا تتجاوز 7 أيّام بعد الإطلاق. يجب إصلاح الثغرات عالية الأهميّة المكتشَفة خلال التقييم وتطبيق ملفات التصحيح عليها في غضون 30 يوماً من الإطلاق. أما الثغرات متوسّطة ومتدنّية الأهميّة فيمكن إصلاحها وتطبيق ملفات التصحيح عليها في غضون 70 يوماً تقويمياً.

ح. أن يجري اختبارات اختراق عامة داخليّة وخارجيّة أقلّه مرة في السنة وبعد أي تغيير أو تحديث ملحوظ في البنى التحتيّة أو في التطبيق.

ط. أن يزيل البرمجيات غير المصرّح لها والمكتشَفة في أنظمة الطرف الثالث أو يعلّق العمل بها، وأن يطبّق المعايير القياسية المتّبعة للسيطرة على البرمجيّات الخبيثة، ما يشمل تنزيل برامج مضادّة للبرمجيّات الخبيثة على جميع الخدمات والأنظمة والأجهزة التي قد تُستخدَم للوصول إلى بيانات فلاي دبي، وتحديث تلك البرمجيّات دورياً واستخدامها بشكل روتيني. وأن يستخدم برامج مضادّة للفيروسات تكون موثوقة وتطبّق أفضل الممارسات في المجال أينما يكون استخدامها ممكناً وأن يتأكّد من تحديث تعريفات الفيروسات عليها بشكل دوري.

ي. أن يحدّث البرمجيّات بشكل مستمر على جميع الخدمات والأنظمة والأجهزة التي قد تُستَخدم للوصول إلى بيانات فلاي دبي، بما في ذلك صيانة النظام (الأنظمة) التشغيلي(ة) بالشكل المناسب، وتنزيل برامج التصحيح الأمنية المحدّثة بشكل معقول بنجاح عليه(ا).

ك. أن يُسنِد مسؤوليات الإدارة الأمنية في ما يتعلق بإعادة ضبط البرامج التشغيليّة المضيفة لأفراد محدّدين.

ل. أن يغيّر جميع أسماء الحسابات و/أو كلمات المرور من حالتها المبدئيّة

8 .المراقبة

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يحتفظ ببيانات الدخول إلى سجلات بيانات فلاي دبي بهدف اكتشاف الحوادث والاستجابة لها، ما يشمل على سبيل المثال لا الحصر:

i. جميع أشكال وصول الأفراد إلى بيانات فلاي دبي

ii. جميع الإجراءات المتَّخذة من قبل الأفراد الذين يتمتّعون بامتيازات إداريّة أو أساسيّة

iii. جميع أشكال وصول المستخدِمين إلى سجلّات مراجعة الحسابات

iv. محاولات الوصول المنطقيّة غير الصالحة

v. استخدامات آليّات التعرّف والتحقّق والتعديلات التي تطالها

ب. أن يسجّل أنشطة النظام الأوّلي الخاص بأنظمة الطرف الثالث التي تحتوي على أي من بيانات فلاي دبي.

ج. أن يحدّ إمكانية الوصول إلى السجلّات الأمنيّة بالأفراد المصرّح لهم وأن يحمي السجلّات الأمنيّة من التعديلات غير المصرّح بها

د. أن يطبّق آليّة كشف التغيّرات (مثلاً مراقبة سلامة الملفّات) لإبلاغ أفراد الطاقم بالتعديلات غير المصرّح بها على ملفّات النظام الهامّة، أو ملفّات الإعداد، أو ملفّات المحتوى؛ أن يُعدّ البرنامج ليقارن بين الملفّات بشكل ضروري أسبوعياً.

هـ. أن يعيد النظر في جميع سجلّات مراجعة الحسابات المتعلّقة وغير المتعلقة بالأمن للأنظمة التي تحتوي على بيانات فلاي دبي أسبوعياً لاكتشاف العيوب وتوثيقها وحلّ جميع المشاكل الأمنيّة المسجّلة في الوقت المناسب.

و. أن يراجع يومياً كلّ الأحداث الأمنية والسجلّات الخاصّة بتخزين عناصر النظام لبيانات حامل البطاقة، أو معالجتها، أو نقلها، فضلاً عن السجّلات الخاصة بعناصر النظام الهامة، والسجلّات الخاصة بعناصر الخوادم والنظام التي تؤدّي وظائف الأمن.

9. بوابات الأمن

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يطلب آلية تحقّق قويّة لإمكانية الوصول الإداري و/أو الإشرافي إلى بوابات الأمن، بما في ذلك، على سبيل المثال لا الحصر، إمكانية الوصول لغرض مراجعة ملفّات السجل.

ب. أن يمتلك عناصر تحكّم وسياسات وعمليات وإجراءات موثّقة ويستخدمها ليضمن عدم تمكّن المستخدمين غير المصرّح لهم بالوصول الإداري و/أو الإشرافي إلى بوابات الأمن، ويضمن ملاءمة مستويات التصريح التي تُمنح للمستخدم ليتمكّن من إدارة بوابات الأمن والإشراف عليها.

ج. أن يتأكّد، أقلّه مرة واحدة كل ستة (6) أشهر، من تعزيز إعدادات بوابة الأمن عن طريق تحديد عيّنة منها والتحقّق من أنّ كلّ مجموعة من القواعد الافتراضية ومعلومات الإعدادات تضمن ما يلي:

i. تعطيل مسار مصدر بروتوكول الإنترنت،

ii. حظر عنوان الاسترجاع من دخول الشبكة الداخلية،

iii. تطبيق المرشحات المضادة للخداع،

iv. منع طرود البث من الدخول إلى الشبكة،

v. تعطيل عمليات إعادة توجيه بروتوكول رسائل التحكم في الإنترنت،

vi. انتهاء مفعول كلّ القواعد بمجرد الضغط على عبارة "رفض الكل"،

vii. إمكانية إرجاع كل قاعدة إلى طلب عمل معين.

د. أن يضمن استخدام أدوات المراقبة للتحقّق من أن كلّ عناصر بوابات الأمن (مثل الأجهزة والبرامج الثابتة والبرمجيات) تعمل بشكل مستمر.

هـ. أن يتأكّد من أنّ جميع بوابات الأمان قد تمّ إعدادها وتطبيقها بشكل يتيح لجميع بوابات الأمن غير العاملة أن تمنع جميع عمليات الوصول.

و. يجب أن تُلغى الطرود الواردة من شبكة خارجية غير موثوق بها داخل المنطقة منزوعة السلاح ("DMZ")، ولا يجوز لها الدخول مباشرة عبر الشبكة الداخلية الموثوقة. يجب أن تنشأ جميع الطرود الواردة التي تدخل إلى الشبكة الداخلية الموثوقة في المنطقة منزوعة السلاح فحسب. ويجب فصل هذه المنطقة عن الشبكة الخارجية غير الموثوق بها عبر بوابة الأمن، كما يجب فصلها عن الشبكة الداخلية الموثوقة عبر أيٍّ من:

i. بوابة أمن أخرى، أو

ii. بوابة الأمن نفسها المستخدمة لفصل المنطقة منزوعة السلاح عن الشبكة الخارجية غير الموثوق بها. في هذه الحالة يجب أن تضمن بوابة الأمن أنّ الطرود المستلمة من الشبكة الخارجية غير الموثوق بها إما تمّ حذفها على الفور أو، في حال عدم حذفها، يتم توجيهها إلى المنطقة منزوعة السلاح فقط من دون معالجة هذا النوع من الطرود إلّا لتدوينها في السجل.

ز. يجب أن تكون العناصر التالية موجودة فقط داخل الشبكة الداخلية الموثوقة:

i. أيّ من بيانات فلاي دبي التي يتم تخزينها من دون استخدام التشفير القوي،

ii. نسخة رسمية عن سجل المعلومات

iii. خوادم قواعد البيانات،

iv. كلّ السجلات المصدّرة

v. كلّ البيئات المستخدمة للتطوير والاختبار وصندوق الحماية والإنتاج وأي بيئات أخرى من هذا القبيل، وكل نسخ الشيفرات الأصلية.

ح. أن يضمن ألّا تكون اعتمادات التحقّق غير المحمية عبر التشفير القوي موجودةً داخل المنطقة منزوعة السلاح

10. أمن الشبكة

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يزوّد شركة فلاي دبي، بناءً على طلب منها، بمخطّط منطقي للشبكة يوثّق الأنظمة والروابط الخاصة بالموارد الأخرى بما في ذلك أجهزة التوجيه والمفاتيح وجدران الحماية والأنظمة الرقمية المتكاملة وطبولوجيا الشبكة ونقاط الاتصال الخارجية والبوابات والشبكات اللاسلكية وأي أجهزة أخرى تدعم فلاي دبي.

ب. أن يحافظ على عملية رسمية يندرج في إطارها الموافقة والاختبار والتوثيق لجميع اتصالات الشبكة والتغييرات التي تطرأ على جدار الحماية وإعدادات أجهزة التوجيه، وأن يعدّ جدران الحماية لتكافح الطرود المشبوهة وتسجّلها، وأن يقيد دورها لتسمح بمرور الطرود المناسبة والمصرح بها دون سواها، مما يمنع كل حركات المرور الأخرى عبر جدار الحماية. ويجب أن يراجع قواعد جدار الحماية كل ستة أشهر.

ج. أن ينشئ جدار حماية عند كل وصلة إنترنت وبين أي منطقة منزوعة السلاح ومنطقة الشبكة الداخلية.

يجب على أي نظام يخزّن المعلومات الشخصية أن يكون موجوداً ضمن منطقة الشبكة الداخلية، ومنفصلاً عن المنطقة منزوعة السلاح (DMZ) والشبكات الأخرى غير الموثوق بها.

د. أن يراقب جدار الحماية عند الحدود الخارجية وفي الداخل للتحكّم بحركة المرور في الشبكة التي تدخل عبرها الطرود أو تغادر الحدود أو الحواجز، وحماية حركة المرور هذه، بحسب الضرورة.

هـ. أن يضمن تطبيق عملية وضوابط موثّقة تعمل على اكتشاف المحاولات غير المصرّح لها للوصول إلى بيانات فلاي دبي، ومعالجتها.

و. أن يحمي بيانات فلاي دبي عند تقديم الخدمات والمنتجات القائمة على شبكة الإنترنت وذلك من خلال تطبيق شبكة منزوعة السلاح. يجب على خوادم الويب التي تقدّم الخدمات لفلاي دبي أن تكون موجودةً في المنطقة منزوعة السلاح. يجب على أي نظام أو مصدر معلومات يخزّن بيانات فلاي دبي (مثل خوادم التطبيقات وقواعد البيانات) أن يكون موجوداً في شبكة داخلية موثوقة. يجب على الطرف الثالث استخدام المنطقة منزوعة السلاح لخدمات شبكة الإنترنت ومنتجاتها.

ز. أن يقيّد وجود الحركة غير المصرّح بها الناتجة عن معالجة التطبيقات أو تخزينها أو نقلها لبيانات فلاي دبي إلى عناوين بروتوكول الإنترنت داخل المنطقة منزوعة السلاح وشبكة الإنترنت.

ح. عند استخدام تقنيات الشبكات اللاسلكية القائمة على الموجات الكهرومغناطيسية لتقديم أو دعم الخدمات والمنتجات لفلاي دبي، يجب على الطرف الثالث أن يتأكّد من أنّ جميع بيانات فلاي دبي المرسلة محمية باستخدام تقنيات تشفير مناسبة كافية لحماية سريّة بياناتها، شرط أن يستخدم هذا التشفير ما لا يقلّ عن أطوال مفتاح 256 بِت للتشفير المتماثل و2048 بت للتشفير غير المتماثل. ويجب أن يمسح بانتظام نقاط الوصول اللاسلكية غير المصرح بها ويحدّدها ويعطّلها.

11 .شروط الاتصال بالبيانات

في حال يتمتّع الطرف الثالث بإمكانية الاتصال بمصادر بيانات فلاي دبي أو يحتاج إلى منحه تصريحاً بالوصول إليها بالتزامن مع الاتّفاقية، وإذا كان الطرف الثالث يتمتّع بإمكانية الاتصال ببيئة فلاي دبي، فيجب على الطرف الثالث، كحد أدنى:

أ. أن يستخدم المرافق ومنهجيات الاتّصال المتّفق عليها برضى الطرفَين فحسب لربط بيئة فلاي دبي مع موارد الطرف الثالث.

ب. ألّا ينشئ رابطاً يصله ببيئة فلاي دبي من دون الحصول على موافقة خطية مسبقة من الشركة.

ج. أن يزوّد فلاي دبي بإمكانية الوصول إلى أي منشآت سارية تابعة له خلال ساعات العمل العادية بهدف صيانة ودعم أي معدات (مثل جهاز التوجيه) توفّرها فلاي دبي بموجب الاتفاقية بهدف تأمين إمكانية الاتصال بمصادر بياناتها.

د. أن يستخدم أي معدات توفرها فلاي دبي بموجب الاتفاقية للاتصال ببيئة فلاي دبي فحسب وذلك بهدف توفير تلك الخدمات والمنتجات أو الوظائف المصرح بها بشكل صريح في الاتّفاقية.

هـ. إذا كانت منهجية الاتصال المتّفق عليها تتطلب أن يقوم الطرف الثالث بتطبيق بوابة أمن، يجب أن يحتفظ بسجلات كلّ الجلسات عبر بوابة الأمن هذه. يجب أن تتضمّن سجلّات الجلسة هذه معلومات مفصّلة تحدّد المستخدم النهائي أو التطبيق النهائي، وعنوان بروتوكول الإنترنت الأصلي، وعنوان بروتوكول الإنترنت الخاص بالوجهة، والمنافذ/بروتوكولات الخدمة المستخدمة ومدّة الوصول. يجب الاحتفاظ بسجلات الجلسة لمدة ستّة (6) أشهر على الأقل من تاريخ إنشاء الجلسة.

و. أن يعلّق أو ينهي فوراً أي توصيل بيني مع بيئة فلاي دبي بناءً على اعتقاد الأطراف الثالثة بحدوث خرق أو وصول غير مصرح به، أو بناءً على تعليمات فلاي دبي إذا تعتقد، وفقًا لتقديرها الخاص، أنّ ثمة خرق للأمن أو وصول غير مصرح به إلى بياناتها أو أيضاً إساءة استخدام مرافق أو أي معلومات أو أنظمة أو موارد أخرى تابعة لها.

12. الهواتف المحمولة والأجهزة المحمولة

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يستخدم التشفير القوي لحماية بيانات فلاي دبي المنقولة التي يتم استخدامها أو الوصول إليها عن بُعد عبر هواتف محمولة وأجهزة محمولة تراعي الشبكة.

ب. عند استخدام هواتف محمولة وأجهزة محمولة تراعي الشبكة، غير أجهزة الكمبيوتر المحمولة، للوصول إلى بيانات فلاي دبي و/أو تخزينها، يجب أن تكون هذه الأجهزة قادرة على حذف جميع النسخ المخزّنة عن بيانات فلاي دبي عند استلام أمر مصدّق عبر الشبكة. (ملاحظة: غالباً ما يشار إلى هذه الإمكانية بقدرة "المسح عن بُعد".)

ج. أن يطبّق سياسات وإجراءات ومعايير موثّقة ليضمن أنّ الطرف المصرّح له، الذي يتولّى مسؤولية الهواتف المحمولة والأجهزة المحمولة المراعية للشبكة، باستثناء كمبيوتر محمول، والذي يخزّن بيانات فلاي دبي سيبدأ فوراً بحذف جميع بيانات فلاي دبي في حال فقدان الجهاز أو سرقته.

د. أن يطبّق سياسات وإجراءات ومعايير موثّقة ليضمن أنّ الهواتف المحمولة والأجهزة المحمولة، غير أجهزة الكمبيوتر المحمولة وغير المراعية للشبكة، ستحذف تلقائياً كلّ النسخ المخزّنة من بيانات فلاي دبي بعد محاولات متتالية وفاشلة لتسجيل الدخول.

هـ. أن يطبّق سياسات وإجراءات ومعايير موثقة تضمن أنّ أي هواتف محمولة وأجهزة محمولة مستخدمة للوصول إلى بيانات فلاي دبي و/أو تخزينها:

i. تعود ملكيتها الفعلية إلى الأطراف المصرّح لها;

ii. تتمّ حمايتها مادياً عندما لا تكون في حوزة الأطراف المصرح لها، أو

iii. يتمّ حذف بياناتها المخزّنة على الفور وبشكل آمن عندما لا تكون في الحيازة المادية لطرف مصرّح له، أو عندما لا تكون محمية مادياً، أو بعد 10 محاولات وصول غير ناجحة.

و. قبل السماح بالوصول إلى بيانات فلاي دبي المخزّنة على الهواتف المحمولة أو الأجهزة المحمولة، أو المخزّنة عبر استخدامها، يجب أن يمتلك الطرف الثالث ويستخدم عملية محدّدة ليضمن ما يلي:

i. أن يكون المستخدم طرفاً مصرحاً له لمثل عملية الوصول هذه،

ii. أن يتمّ التحقّق من هوية المستخدم.

ز. أن يطبّق سياسة تحظر استخدام أي هواتف محمولة أو أجهزة محمولة تخضع لإدارة و/أو إشراف الطرف الثالث أو فلاي دبي للوصول إلى بيانات فلاي دبي و/أو تخزينها.

ح. أن يراجع على الأقل مرة سنوياً طريقة استخدام وضوابط جميع الهواتف والأجهزة المحمولة التي تخضع لإدارة الطرف الثالث أو إشرافه للتأكّد من أنّ الهواتف المحمولة والأجهزة المحمولة تمتثل لتدابير الأمن التقنية والتنظيمية المعمول بها.

13 .الأمن في المرور

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يستخدم التشفير القوي لنقل بيانات فلاي دبي خارج الشبكات التي تديرها فلاي دبي أو الطرف الثالث، أو عند نقل بيانات فلاي دبي عبر أي شبكة غير موثوق بها.

ب. بالنسبة إلى السجلات التي تحتوي على بيانات فلاي دبي على شكل أوراق أو بطاقات مجهرية أو وسائط إلكترونية بهدف نقلها فعلياً، يجب على الطرف الثالث أن ينقلها عن طريق البريد الآمن أو أي طريقة تسليم أخرى يمكن تتبّعها وتعبئتها بشكل آمن وفقاً لمواصفات الشركة المصنّعة. يجب نقل أي بيانات خاصة بفلاي دبي في حاويات مقفلة.

14 .الأمن خارج أوقات العمل

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يستخدم التشفير القوي لحماية بيانات فلاي دبي عند تخزينها.

ب. ألّا يخزّن بيانات فلاي دبي إلكترونياً خارج شبكة الطرف الثالث (أو شبكة الكمبيوتر الآمنة الخاصة بفلاي دبي) ما لم يكن جهاز التخزين (على سبيل المثال، شريط النسخ الاحتياطي أو الكمبيوتر المحمول، أو شريحة الذاكرة، أو قرص الكمبيوتر، وغيرها) محمياً عبر التشفير القوي.

ج. ألّا يخزّن بيانات فلاي دبي على وسائط قابلة للإزالة (ذاكرات التخزين الخارجية المحمولة أو شرائح الذاكرة أو الأشرطة أو الأقراص المضغوطة أو محركات الأقراص الصلبة الخارجية) باستثناء: لأغراض النسخ الاحتياطي واستمرارية الأعمال ومواجهة الأزمات وتبادل البيانات على النحو المسموح به والمطلوب بموجب العقد المُبرَم بين الطرف الثالث وفلاي دبي. إذا تم استخدام الوسائط القابلة للإزالة لتخزين المعلومات الشخصية أو المعلومات السرية وفقاً للاستثناءات المذكورة في هذا القسم الفرعي، ينبغي حماية المعلومات باستخدام التشفير القوي. يجب تعطيل "التشغيل التلقائي" للوسائط القابلة للإزالة وأجهزة التخزين.

د. أن يخزّن السجلات التي تحتوي على بيانات فلاي دبي على شكل أوراق أو بطاقات مجهرية في المناطق التي يقتصر الوصول إليها على الأفراد المصرح لهم، ويحمي هذه السجّلات.

هـ. أن يضمن أن تكون المعلومات شخصية أو سريّة، عند جمع بيانات فلاي دبي أو إصدارها أو إعدادها على شكل أوراق ونسخ احتياطية من قبل فلاي دبي أو بواسطتها أو بالنيابة عنها أو باسم علامة فلاي دبي، ما لم تصدر فلاي دبي تعليمات خطية بخلاف ذلك، وأن يحدّد هذه المعلومات الخاصة بفلاي دبي على أنّها "سرية". يقرّ الطرف الثالث بأن بيانات فلاي دبي تعود ملكيتها إلى فلاي دبي وستبقى كذلك، بغض النظر عن التسميات أو غيابها.

15 .الإرجاع والاحتفاظ والتلف والمسح

يجب على الطرف الثالث، كحدّ أدنى:

أ. من دون أن تترتّب أي رسوم إضافية على فلاي دبي، وبناءً على طلب فلاي دبي أو عند إنهاء الاتفاقية، أن يقدّم نسخاً عن أي من بيانات فلاي دبي إلى فلاي دبي في غضون ثلاثين (30) يوماً من تاريخ إصدار هذا الطلب أو إنهاء الاتفاقية. يجب على الطرف الثالث إرجاع جميع بيانات فلاي دبي أو تلفها، بما في ذلك النسخ الاحتياطية الإلكترونية والصلبة والآمنة على النحو المنصوص عليه في انتهاء (i) :الاتفاقية، أو إذا ما كان منصوصاً عليها في الاتفاقية بجب تلفها أو إرجاعها في غضون تسعين (90) يوماً من أقرب فترة لـ التاريخ الذي لم يعد فيه الطرف الثالث بحاجة إلى بيانات (iii) من طلب فلاي دبي بإعادة بياناتها، أو (ii)صلاحية الاتفاقية أو إنهائها، فلاي دبي لأداء التزاماته ومنتجاته بموجب الاتفاقية.

ب. في حال موافقة فلاي دبي على التلف كبديل عن إعادة بياناتها، أن يشهد كتابةً من قبل مسؤول من الطرف الثالث بأن التلف يجعل بيانات فلاي دبي غير قابلة للاسترداد وغير قابلة للاسترداد. ويجب على الطرف الثالث أن يتلف جميع نسخ بيانات فلاي دبي في جميع المناطق وفي جميع الأنظمة التي تُخزّن فيها، بما في ذلك على سبيل المثال لا الحصر الأطراف المصرّح لها مسبقاً. يجب تلف هذه المعلومات باتباع إجراء قياسي صناعي للتلف الكامل مثل برنامجَي NIST Special Publication 800-88 أو DOD 5220.22M باستخدام منتج مسح مغناطيسي موصى به من قبل الشركة المصنّعة للنظام المتأثر. قبل إجراء عملية التلف، يجب على الطرف الثالث الحفاظ على جميع التدابير الأمنية التقنية والتنظيمية المعمول بها لحماية أمن بيانات فلاي دبي وخصوصيتها وسريتها.

ج. أن يمسح المعلومات الشخصية ومعلومات فلاي دبي السريّة بطريقة تضمن عدم إعادة استرجاع المعلومات وإعادة استخدامها. يجب التخلص من الأوراق والشرائح والميكروفيلم والبطاقات المجهرية والصور عن طريق تقطيعها بالكامل أو حرقها. يجب تخزين المواد التي تحتوي على بيانات فلاي دبي التي يجب تلفها في حاويات آمنة، ويجب نقلها باستخدام طرف ثالث آمن.

16. الاستجابة للحوادث والإخطار بها

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يمتلك عملية لإدارة الحوادث ويعتمدها، إلى جانب إجراءات ذات الصلة وموظفين مثل عملية إدارة الحوادث والإجراءات التي تتمتّع بموارد متخصّصة. ويجب عليه فوراً، وفي غضون فترة لا تتعدّى أربعاً وعشرين (24) ساعة، أن يخطر فلاي دبي متى حصل أي هجوم مشتبه به أو مؤكد، أو تسلّل، أو وصول غير مصرح به، أو فقدان، أو أي حادث آخر يطرأ على معلومات فلاي دبي أو أنظمتها أو مواردها الأخرى.

ب. أن يزوّد فلاي دبي بعد إخاطرها بتحديثات منتظمة عن الحالة، بما في ذلك، على سبيل المثال لا الحصر، الإجراءات المتّخذة لحل هذا الحادث على فترات أو أوقات متّفق عليها من قبل الطرفَين طوال مدّة الحادث وفي أقرب وقت ممكن ومعقول بعد حلّ الحادث، ويجب عليه أن يزوّد فلاي دبي بتقرير خطي يصف فيه الحادث والإجراءات التي اتّخذها الطرف الثالث في إطار الاستجابة للحادث والخطط التي اعتمدها حيال الإجراءات المستقبلية التي سيعتمدها لمنع وقوع حادث مماثل.

ج. ألّا يبلغ عن أي خرق يطال معلومات فلاي دبي أو أنظمتها أو مواردها الأخرى أو يكشف عنه علناً من دون إخطار فلاي دبي أولاً والعمل مباشرةً معها لإخطار المسؤولين الحكوميين على مستوى الإقليم أو الدولة أو الولاية أو المستوى المحلي أو المسؤولين عن خدمات مراقبة الائتمان، فضلاً عن الأفراد المتضرّرين من هذا الخرق، وأي منافذ إعلامية سارية، وفقًا لما يقتضيه القانون.

د. أن يطبّق عملية لتحديد انتهاكات الضوابط الأمنية على الفور بما في ذلك الضوابط التي نصّت عليها الأطراف الثالثة في هذه السياسة. يخضع المخالفون الذين يتم تحديد هويتهم للإجراءات التأديبية المناسبة بموجب القوانين المعمول بها. على الرغم مما سبق، يظل المخالفون تحت سلطة الأطراف الثالثة. لا تُعتبر شركة فلاي دبي ربة عمل بالنسبة إلى الطرف الثالث.

17. إدارة استمرارية الأعمال والتصدي للأزمات

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يطوّر الخطط الموضوعة لضمان استمرارية العمل في كل منطقة والخطط الموضوعة للتصدي للأزمات في كل تكنولوجيا أساسية، كما يجب أن يشغّلها ويديرها ويراجعها بهدف تقليص التأثير على فلاي دبي الذي يرتبط بأداء الطرف الثالث ولا سيما بأداء موجباته المنصوص عليها في هذه الاتفاقية. يجب أن تشمل هذه الخطط ما يلي: الموارد المحدّدة الخاصة بوظائف استمرارية الأعمال والتصدي للأزمات، والأهداف المحدّدة لمدّة التصدّي للأزمات المحددة ونقطة التصدي لها، والنسخ الاحتياطية اليومية عن البيانات والأنظمة، والتخزين خارج الموقع للوسائط الاحتياطية والسجلّات، وحماية السجلّات وخطط الطوارئ المتناسبة وفقًا لشروط الاتّفاقية، ويجب أن يخزّن هذه الخطط بأمان خارج الموقع وأن يضمن توفّر هذه الخطط للطرف الثالث عند الحاجة.

ب. أن يزوّد فلاي دبي، بناءً على طلب منها، بخطة موثّقة لاستمرارية الأعمال تضمن أن يفي الطرف الثالث بموجباته التعاقدية المنصوص عليها بموجب الاتفاقية وهذه الوثيقة، بما في ذلك شروط قابلة للتطبيق تعود لأي بيان عمل أو اتّفاقية على مستوى العمل أو الخدمة. يجب أن تتصدّى هذه الخطط للأزمات مع حماية سلامة بيانات فلاي دبي وسريتها.

ج. أن يمتلك إجراءات موثقة للنسخ الاحتياطية عن بيانات فلاي دبي وخطط استعادتها ويجب أن تشمل على الأقل إجراءات نقل النسخ الاحتياطية عن بيانات فلاي دبي وتخزينها وتلفها، ويجب أن يقدّم هذه الإجراءات الموثّقة إلى شركة فلاي دبي بناءً على طلب منها.

د. أن يضمن إنشاء نسخ احتياطية عن كلّ بيانات فلاي دبي المخزّنة أو البرامج والإعدادات الخاصّة بالأنظمة التي تستخدمها فلاي دبي على الأقلّ مرة واحدة أسبوعياً.

هـ. أن يطبّق هذه الخطط بشكل شامل على حساب الطرف الثالث ونفقته الخاصة، وذلك بشكل منتظم، لكن لا يتعدّى المرّة الواحدة سنوياً، أو بعد أي تغيير جوهري يطرأ على خطّة استمرارية الأعمال أو خطط التصدي للأزمات. يجب أن تضمن هذه الممارسات الأداء السليم للتقنيات المتضرّرة وتزيد الوعي الداخلي بهذه الخطط. يجب تحديث خطط استمرارية الأعمال والتصدّي للأزمات على الأقل مرّة واحدة سنوياً، أو كلما دعت الحاجة بسبب تغييرات كبيرة تطرأ على بيئة الأعمال و/أو التكنولوجيا.

و. أن يراجع على الفور خطة استمرارية الأعمال الخاصة به لمعالجة المصادر أو السيناريوهات الإضافية أو الناشئة التي تشكّل تهديداً وأن يقدّم لفلاي دبي ملخصاً عالي المستوى يضمّ الخطط والاختبارات المتّبعة عند الطلب في غضون إطار زمني معقول.

ز. أن يضمن أنّ جميع المناطق التابعة للطرف الثالث أو المناطق المتعاقد عليها مع الطرف الثالث، التي تحتوي على بيانات فلاي دبي أو تعالجها، تخضع للمراقبة على مدار 24 ساعة في اليوم، وسبعة (7) أيام في الأسبوع لمكافحة التسلّل والحرائق والمياه والمخاطر البيئية الأخرى.

18. الامتثال والاعتمادات

يجب على الطرف الثالث، كحدّ أدنى:

أ. أن يحتفظ بسجلات كاملة ودقيقة ترتبط بأدائه موجباته المنصوص عليها في هذه السياسة وامتثاله لها بشكل يسمح بالتقييم أو التدقيق لمدة لا تقل عن ثلاث (3) سنوات أو أكثر وفقاً للشروط المطلوبة بموجب أمر محكمة أو إجراء مدني أو تنظيمي. على الرغم ممّا سبق ذكره، يجب على الطرف الثالث الاحتفاظ بسجلات الأمن لمدة عام واحد (1) على الأقل بعد أي تطبيق مستمر للاتفاقية.

ب. أن يسمح لفلاي دبي، من دون فرض أي تكلفة إضافية، بإجراء تقييمات أمنية دورية أو عمليات تدقيق للتدابير الأمنية الفنية والتنظيمية التي يعتمدها الطرف الثالث، إذ يجب على فلاي دبي أن تزوّد الطرف الثالث باستبيانات خطية وطلبات للتوثيق. بالنسبة إلى جميع الطلبات، يجب على الطرف الثالث أن يجيب على الفور كتابةً مع إرفاق أدلة، إن أمكن، أو بناءً على اتفاق متبادل. يتعين على الطرف الثالث جدولة تدقيق أمني ليبدأ في غضون عشرة (10) أيام عمل من طلب فلاي دبي لإجراء تدقيق. قد تطلب فلاي دبي الوصول إلى المرافق أو الأنظمة أو العمليات أو الإجراءات لتقيّم بيئة الرقابة الأمنية الخاصة بالطرف الثالث.

ج. أن يصدّق على امتثاله لهذه الاتفاقية بناءً على طلب فلاي دبي مع إرفاق أحدث شهادات عن ISO 27001/27002 أو PCI-DSS أو SOC 2 لإثبات ذلك، أو إرفاق أي تقييم مشابه يختصّ بالطرف الثالث وأي مقاول فرعي أو طرق المعالجة أو طرق الوصول أو التخزين أو الإدارة التي يعتمدها طرف ثالث نيابةً عن الطرف الثالث. إذا لم يستطع الطرف الثالث التصديق على الامتثال، فيجب عليه تقديم تقرير خطي يوضح فيه بالتفصيل نقاط عدم الامتثال للاتفاقية وخطة المعالجة التي ينوي اتباعها ليمتثل بها.

د. في حال رأت فلاي دبي، وفقاً لتقديرها الخاص، أنّ خرقاً أمنياً قد حدث ولم يتمّ إبلاغها عنه كما هو منصوص عليه في هذه الاتفاقية وفي عمليّة إدارة الحوادث الخاصّة بالطرف الثالث، يجب أن يُحدّد موعداً للتدقيق أو التقييم يبدأ في غضون أربعة وعشرين (24) ساعة من استلام الإخطار الذي تطلب فلاي دبي بموجبه القيام بتقييم أو تدقيق.

ه. أن يقدّم إلى فلاي دبي، في غضون ثلاثين (30) يوماً تقويمياً من استلام نتائج التقييم أو تقرير التدقيق، تقريراً خطّياً تُحدّد فيه الإجراءات التصحيحيّة التي نفّذها الطرف الثالث أو يقترح تنفيذها مرفقاً بجدولٍ زمني لكلّ إجراء تصحيحي ووضعه الحالي. يتعيّن على الطرف الثالث أن يحدّث هذا التقرير ويقدّمه إلى فلاي دبي كلّ ثلاثين (30) يوماً تقويمياً للإبلاغ عن حالة كافة الإجراءات التصحيحيّة حتى تاريخ تنفيذها. يتعيّن على الطرف الثالث تنفيذ كافة الإجراءات التصحيحيّة في غضون تسعين (90) يوماً من استلامه تقرير التقييم أو التدقيق أو خلال فترة زمنيّة بديلة، شرط أن يتّفق الطرفان على هذه الفترة الزمنيّة البديلة خطّياً في غضون فترة لا تتعدّى ثلاثين (30) يوماً من تاريخ استلام الطرف الثالث لتقرير التقييم أو التدقيق.

و. أن يمتثل ويبقى ممتثلاً لأيّ معايير مطبّقة مرتبطة بأمن المعلومات التي تفرضها الحكومة

ويتعيّن على الطرف الثالث تولي الأمور المرتبطة بحسابات الدفع من أرقام .ISO 27001/27002 وشروط إعداد التقارير ومعيار ليغطي (PCI-DSS) حسابات أو أي معلومات دفع أخرى ذات صلة، فضلاً عن الامتثال لأحدث نسخة صادرة عن قطاع بطاقات الدفع كافة الأنظمة التي تتعامل مع هذه المعلومات ويجب أن يحافظ على هذا الامتثال. في حال لم يعد الطرف الثالث ممتثلاً لأي نظام ، يجب على الطرف الثالث إخطار فلاي دبي على PCI من الأنظمة التي تتعامل مع البيانات المطبقة على PCI-DSS مرتبط ببطاقة الفور، وأن يعمل على الفور ومن دون أي تأخير على معالجة عدم امتثاله، وأن يطلع فلاي دبي بانتظام على مسار هذه المعالجة عند الطلب.

19 .المعايير، وأفضل الممارسات، والأنظمة، والقوانين

في حال قام الطرف الثالث بمعالجة بيانات فلاي دبي أو الوصول إليها أو الاطلاع عليها أو تخزينها أو إدارتها، ونعني بذلك البيانات التي تتعلّق بموظّفي فلاي دبي وشركائها والشركات التابعة لها وعملائها، أو التي تتعلّق بموظفي فلاي دبي أو المقاولين أو المقاولين الثانويّين أو الموردين، يجب أن يتّخذ الطرف الثالث تدابير أمنيّة على المستويين التقني والتنظيمي لا تقل صرامةً عمّا تنصّ عليه الإرشادات والأنظمة والتوجيهات والقوانين العالميّة والإقليميّة والوطنيّة والمحليّة المعمول بها.