سياسة أمان المعلومات

1. الهدف

تهدف سياسة أمان المعلومات إلى وضع خارطة طريق لتنفيذ تدابير الأمان لحماية أصول شركة جيلجامش للخدمات المالية و/أو GFX Securitiesو/أو الشركة الأكثر قيمة. يجب أن تحدد سياسة الأمان القوية نبرة الأمان لجميع أفراد شركة جيلجامش للخدمات المالية و/أو GFX Securitiesو/أو الشركة، وتوضح لهم ما هو متوقع منهم. يجب على جميع الأفراد أن يكونوا على علم بحساسية البيانات ومسؤولياتهم في حمايتها.

---

2. النطاق

تنطبق هذه السياسة على جميع الأفراد في مجموعةGFX INVESTMENT LIMITED ، بما في ذلك الموظفين بدوام كامل وبدوام جزئي، الموظفين المؤقتين، المقاولين، والاستشاريين الذين يكونون "مقيمين" في موقع الكيان أو لديهم وصول إلى بيئة بيانات حاملي البطاقات.

المسؤوليات

- مسؤول الشبكة
- مسؤول النظام
- مالك العملية
- فريق تطوير تكنولوجيا المعلومات
- فريق البنية التحتية لتكنولوجيا المعلومات

---

3. بيان السياسة

يجب على مجموعة GFX INVESTMENT LIMITED اتباع السياسة الموضحة:

- يجب حماية المعلومات والأصول التكنولوجية من الوصول غير المصرح به.
- المعلومات متاحة على أساس الحاجة إلى المعرفة فقط.
- لا يتم الكشف عن المعلومات للأشخاص غير المصرح لهم من خلال إجراءات متعمدة أو غير مبالية.
- يتم ضمان سرية المعلومات وفقًا للاتفاقيات وأفضل الممارسات في شركة جيلجامش للخدمات المالية و/أو GFX Securities و/أو الشركة.
- يتم حماية المعلومات من التعديل غير المصرح به.
- يتم الوفاء بمتطلبات اللوائح والتشريعات المعمول بها.
- يتم تطوير وصيانة واختبار خطط استرداد الكوارث للأصول التكنولوجية بقدر الإمكان.
- يتولى المسؤول التنفيذي المسؤولية المباشرة عن الحفاظ على السياسة وتقديم التوجيه بشأن تنفيذها.
- يجب على شركة جيلجامش للخدمات المالية و/أو GFX Securities و/أو الشركة التأكد من أن سياسة وإجراءات الأمان تحدد بوضوح مسؤوليات أمان المعلومات لجميع الأفراد. يجب تعيين فرد أو فريق للقيام بالمسؤوليات التالية في إدارة أمان المعلومات:

- وضع وتوثيق وتوزيع سياسات وإجراءات الأمان.
- مراقبة وتحليل تنبيهات وأخبار الأمان، وتوزيعها على الأفراد المناسبين.
- وضع وتوثيق وتوزيع إجراءات استجابة للأحداث الأمنية وتصعيدها لضمان التعامل الفوري والفعال مع جميع الحالات.
- إدارة حسابات المستخدمين، بما في ذلك الإضافات والحذف والتعديلات.
- مراقبة والتحكم في جميع الوصول إلى البيانات.
- يتم تقديم تدريب على أمان المعلومات لجميع المستخدمين عند التوظيف وعند كل سنة.
- يتم الإبلاغ والتحقيق في جميع خروقات أمان المعلومات، سواء كانت فعلية أو مشتبه بها.
- يتحمل جميع رؤساء الأقسام/قادة الفرق المسؤولية المباشرة عن تنفيذ السياسة في مجالات أعمالهم/أقسامهم، والامتثال من قبل موظفيهم.
- يتم الدعوة وتعزيز ثقافة الامتثال تجاه أمان المعلومات.
- يتم التعامل مع انتهاكات السياسات من خلال اتخاذ إجراءات تأديبية.
- يجب مراجعة سياسة أمان المعلومات سنويًا وتحديثها بناءً على أهداف العمل أو بيئة المخاطر.
- يجب على شركة جيلجامش للخدمات المالية و/أو GFX Securities و/أو الشركة فحص جميع الأفراد المحتملين قبل التوظيف لتقليل خطر الهجمات من المصادر الداخلية. (تشمل أمثلة الفحوصات الخلفية تاريخ التوظيف السابق، السجل الجنائي، تاريخ الائتمان، وفحوصات المراجع.)

سياسة نقل البيانات بشكل آمن

1. يجب على خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة استخدام التشفير القوي وبروتوكولات الأمان في جميع المواقع التي يتم فيها نقل أو استقبال بيانات بطاقات حساسة عبر الشبكات العامة المفتوحة، بما في ذلك ما يلي:
   - قبول المفاتيح والشهادات الموثوقة فقط.
   - البروتوكول المستخدم يدعم فقط النسخ أو التكوينات الآمنة.
   - قوة التشفير مناسبة لطريقة التشفير المستخدمة.
2. يجب على خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة التأكد من أن جميع الشبكات اللاسلكية التي تنقل بيانات حاملي البطاقات، البيانات الحساسة، أو المتصلة ببيئة بيانات حاملي البطاقات، تستخدم أفضل الممارسات في الصناعة لتطبيق تشفير قوي للمصادقة والنقل. يجب عدم استخدام WEP لأغراض الأمان.
3. للتنفيذاتTLS ، يجب على خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة التحقق من تفعيل استخدام TLS كلما تم نقل أو استقبال بيانات حاملي البطاقات والبيانات الحساسة.
4. يجب على خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة عدم إرسال أرقام PAN غير المحمية عبر تقنيات الرسائل المستخدمة من قبل المستخدمين النهائيين (على سبيل المثال، البريد الإلكتروني، الرسائل الفورية، الرسائل القصيرة، الدردشة، إلخ).
5. يجب على خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة التأكد من أن السياسات الأمنية والإجراءات التشغيلية لتشفير نقل بيانات حاملي البطاقات والبيانات الحساسة موثقة، ومستخدمة، ومعروفة لجميع الأطراف المعنية.
6. عندما يكون الجهاز المشمول قابلاً للوصول عبر واجهة الويب، يجب أن يتم نقل حركة المرور على الويب عبر Secure Sockets Layer (SSL)، باستخدام بروتوكولات أمان قوية فقط، مثل.(Transport Layer Security (TLS
7. يجب تأمين البيانات المشمولة المرسلة عبر البريد الإلكتروني باستخدام أدوات تشفير بريد إلكتروني قوية تشفيرياً مثل PGP أو S/MIME.
8. يجب تشفير البيانات المشمولة التي يتم نقلها غير الويب عبر تشفير على مستوى التطبيق، أي حيث تقيم قاعدة بيانات التطبيق خارج خادم التطبيق، يجب أيضًا تشفير الاتصال بين قاعدة البيانات والتطبيق.
9. عندما لا يتوفر تشفير على مستوى التطبيق لبيانات غير الويب المشمولة، يجب تنفيذ تشفير على مستوى الشبكة مثل IPsec أو SSH tunneling.

فيما يلي قائمة بالخدمات غير الآمنة جنبًا إلى جنب مع خدمات الأمان البديلة لها:

استخدم...	بدلاً من...
HTTP	وصول الويب
FTP, RCP	نقل الملفات
TELNET	قشرة بعيدة
VNC	سطح مكتب بعيد

حماية البيانات - سرية البيانات

تتخذ الشركة تدابير تتماشى مع قانون حماية البيانات لتنفيذ وصيانة الأنظمة والإجراءات التي تكون كافية لضمان أمان المعلومات وسلامتها وسريتها. أنشأت الشركة آليات أمان لضمان أمان وتوثيق وسائل نقل المعلومات، وتقليل مخاطر فساد البيانات والوصول غير المصرح به ومنع تسرب المعلومات، للحفاظ على سرية البيانات في جميع الأوقات.

جميع المعلومات غير العامة التي يقدمها العملاء إلى الشركة تُحتفظ بسرية ولا يتم الكشف عنها لأي شخص آخر إلا كما يلي:

- بموافقة صريحة من العميل الذي قدم هذه المعلومات؛
- إلى FSC إذا طُلب من الشركة أو كان مطلوباً قانونياً القيام بذلك من قبلFSC ؛
- وفقاً لاكتشاف قانوني مطلوب؛
- إلى طرف مقابل يقدم خدمات المقاصة التي يكون العميل عضواً فيها أو فيما يتعلق بمقاصة الأوراق المالية؛
- مع الالتزام بمتطلبات السرية المناسبة، إلى أي شخص يقدم خدمات للشركة؛
- مع الالتزام بمتطلبات السرية المناسبة، إلى موظفي الشركة، المجلس، لجان المجلس، المحامون، المدققون والوكلاء، المتعهدون المستقلون أو الأشخاص الآخرين الذين تم التعاقد معهم من قبل الشركة، في كل حالة، الذين يحتاجون إلى هذه المعلومات فيما يتعلق بأداء واجباتهم تجاه الشركة؛ و
- يتم التعامل مع جميع المعلومات والبيانات التي يتم الحصول عليها أو استلامها من الشركة من عمليات تفتيش المحاسبة والسجلات الأخرى كسرية من قبل الشركة.

سياسة وإجراءات أمان الشبكة

سوف يتم تعيين المسؤولية العامة عن نشاط إدارة الشبكة إلى فريق عمليات الشبكة. ستُعهد المسؤوليات عن المهام الرئيسية إلى فرد واحد أو أكثر. يجب التأكد من أن استخدام خدمات الشبكة يتوافق مع سياسة إدارة الوصول للمستخدم ومتطلبات تطبيقات الأعمال.

يجب تكوين وصيانة وتأمين مكونات الشبكة والأمان المستخدمة في الاتصال وأمان الشبكة بشكل مناسب.

يجب على خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة استخدام تقنيات كشف التسلل و/أو منع التسلل لاكتشاف و/أو منع التسللات إلى الشبكة. يجب مراقبة كل حركة المرور عند محيط بيئة بيانات حاملي البطاقات وكذلك في النقاط الحرجة في بيئة بيانات حاملي البطاقات، وتنبيه الموظفين إلى المساومات المشتبه فيها. يجب إبقاء جميع محركات كشف التسلل ومنعها، القواعد الأساسية، والتواقيع محدثة.

يجب أن تكون الخوادم التي تدعم التطبيقات الحرجة مفصولة منطقياً عن الخوادم الأخرى. يجب أن يحتوي تصميم الشبكة على تقسيم للشبكة بحيث، على سبيل المثال، ولكن ليس على سبيل الحصر، يجب أن تكون الخوادم التي تدعم التطبيقات الحرجة مفصولة منطقياً عن الخوادم الأخرى. يجب أن تمر جميع الاتصالات بخوادم التطبيقات الحرجة عبر جدار الحماية.

يجب تقييد نقاط الدخول إلى شبكة خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة والتأكد من استخدام جدران الحماية لتأمين هذه النقاط.

يجب تكوين وصيانة وتأمين مكونات الشبكة والأمان المستخدمة في الاتصال وأمان الشبكة بشكل مناسب.

يجب دعم مكونات الشبكة من خلال توثيق دقيق ومحدث، لضمان تكوين الشبكة بدقة وأمان.

يجب تخزين معلومات التكوين الحالية حول بنية الشبكة وأجهزة الشبكة الحيوية مثل جدار الحماية ومكونات النظام محلياً وعمل نسخة احتياطية بشكل آمن في موقع بديل.

يجب أن تكون تكنولوجيا المعلومات مسؤولة عن إنشاء وصيانة اتفاقيات خدمات الشبكة مع الأطراف الخارجية. يجب أن تشمل مثل هذه الاتفاقيات، ولكن قد لا تقتصر على:

- وصف واضح لميزات الأمان
- مستويات الخدمة
- متطلبات إدارة جميع خدمات الشبكة المستخدمة
- شروط عدم الكشف عن معلوماتGFX INVESTMENT GROUP LIMITED
- يجب اتخاذ تدابير كافية لضمان الأمان في جميع الاتصالات البعيدة.

نسخ البيانات الاحتياطية واستعادتها (النسخ الورقية والإلكترونية)

تحافظ خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة على سجلاتها الإلكترونية لدى مقدمي خدمات السحابة ومزودي أنظمة التداول. تشمل هذه السجلات سجلات المحاسبة الداخلية للشركة، واتفاقيات الاشتراك، وسجلات التداول، وما إلى ذلك. إذا كان موقعنا الرئيسي غير قابل للتشغيل، سنواصل العمليات من الموقع الاحتياطي أو موقع بديل باستخدام أجهزة جديدة والاتصال بحساباتنا على الإنترنت مع مقدمي خدمات السحابة.

التكنولوجيا، البيانات وأمن المعلومات

ستحتفظ الشركة بمعلومات معينة تتعلق بالعملاء في قواعد بياناتها الإلكترونية لتسهيل معالجة المعاملات نيابة عن عملائها بما يتماشى مع القواعد واللوائح والقوانين. المعلومات الشخصية القابلة للتحديد المخزنة على شبكة GFX INVESTMENT GROUP LIMITED محمية من الوصول غير المصرح به، وتُعامل على أنها سرية، وتُدار وفقًا لشروط سياسة الخصوصية الخاصة بخدمات جيلجامش المالية و/أو GFX Securitiesو/أو الشركة.

نؤكد أن المعلومات الشخصية القابلة للتحديد ومعلومات العملاء المخزنة على أنظمتنا ستكون محمية على النحو التالي:

- ستكون خوادم الشركة المواجهة للإنترنت محمية من الوصول من خلال جدران الحماية و/أو أجهزة الأمان الأخرى.
- ستقيم الخوادم الحرجة للشركة على شبكات معزولة لن تكون لها وصول مباشر إلى الإنترنت.
- ستقوم الأنظمة الداخلية في خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة التي تخزن معلومات العملاء الشخصية القابلة للتحديد بقفل الوصول بعد عدد قليل من محاولات تسجيل الدخول غير الناجحة.
- سيكون الوصول إلى الأقراص المشتركة مقصورًا على الموظفين النشطين والأفراد المصرح لهم مسبقًا على أساس "الحاجة إلى المعرفة" داخل خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة من خلال تسجيل الدخول المحمي بكلمة مرور إلى الشبكة.
- سيتم استخدام تقنية التشفير لنقل البيانات عبر الشبكات العامة وعلى أجهزة الوسائط المحمولة.
- ستقيم النسخ الاحتياطية للأنظمة إما في مرافق آمنة في خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة أو في تخزين آمن مزود من طرف ثالث متخصص في إدارة المعلومات بشكل آمن.
- ستستخدم جميع أجهزة الكمبيوتر الطرفية برامج مكافحة الفيروسات الحديثة التي يتم تحديثها بانتظام.
- ستُطبق تصحيحات أمان نظام التشغيل على جميع الأنظمة بانتظام.
- سيتم تدريب الموظفين على متطلبات حماية المعلومات الشخصية.
- الأنظمة مصممة بشكل معقول لحماية المعلومات الشخصية القابلة للتحديد.

تؤكد خدمات جيلجامش المالية و/أو GFX Securities و/أو الشركة أنه في حال حدوث خرق، ستتخذ الإدارة فورًا إجراءات لتأمين المعلومات، وتخفيف تأثير الخرق، وإخطار أي عملاء قد تكون معلوماتهم الشخصية القابلة للتحديد قد تعرضت للخطر في الوقت المناسب.

وظيفة تكنولوجيا المعلومات

سيدير القسم المعني وظائف تكنولوجيا المعلومات داخليًا، بينما ستدخل الشركة في اتفاقيات تعاون مع مقدمي الخدمات لضمان الأمان وسلامة:

- الشبكة المستخدمة من قبل الشركة
- منصة التداول التي يستخدمها موظفو الشركة والعملاء
- الخوادم وأجهزة الكمبيوتر الشخصية لموظفي الشركة

بالإضافة إلى ذلك، سيكون القسم بدعمه الخارجي الضروري مسؤولاً عن ضمان وجود إجراءات فيما يتعلق بالقضايا التالية:

- أمان تكنولوجيا المعلومات
- نسخ احتياطي لتكنولوجيا المعلومات

استمرارية أنظمة تكنولوجيا المعلومات

أنشأت إدارة تكنولوجيا المعلومات إجراءات لضمان أنه في حالات انقطاع أنظمة الشركة (التداول، الهواتف، وما إلى ذلك)، يتم تلبية ما يلي:

- الحفاظ على البيانات والوظائف الأساسية.
- الحفاظ على تقديم خدمات واستثمارات الشركة.
- على الأقل، استرداد البيانات والوظائف في الوقت المناسب واستئناف خدمات واستثمارات الشركة في الوقت المناسب.

تحدد الشركة الأنظمة المحددة التي تعتبر أنظمة أساسية لضمان استمرارية الأعمال. تضمن هذه الأنظمة :أ. الوصول المستمر وغير المنقطع إلى الإنترنت .ب. التشغيل المستمر وغير المنقطع لمنصة التداول .ج. التشغيل المستمر وغير المنقطع لنظام الهاتف الرقمي الذي سيكون حاسمًا في سير عمل نظام طلبات الهاتف. يجب أن يكون نظام تقديم طلبات الهاتف بديلاً/نسخة احتياطية للنظام المعتمد على الإنترنت.

إذا، بسبب فشل النظام أو التكامل، كان المستخدم لهذا المستند غير قادر على تنفيذ أي مهام، فيجب الاتصال بالشركة على الفور. إذا لم يتم حل مشكلة النظام على الفور، فيجب أيضًا إبلاغ المؤلف و/أو الموافق على هذه السياسة دون تأخير غير مبرر.

لتقليل التأثير على الأنظمة الحرجة الناتج عن الفشل الأساسي، ستأخذ تصاميم النظام هذه الأنظمة الاحتياطية في الاعتبار طرقًا ووسائل لدعم الانتقال إلى الأنظمة الثانوية.

من أجل ضمان استمرار الأنظمة في العمل بمستويات أداء مناسبة، سيتم جمع ومراقبة مقاييس النظام بواسطة حل مراقبة مركزي. أي خرق لعتبات الأداء سيتم الإبلاغ عنه إلى فريق الخدمة الفنية للمراجعة مع التخطيط لترقيات حيثما كان ذلك مناسبًا. سيتم استضافة أنظمة الشركة، حيثما أمكن، على بنية تحتية سحابية مما يسمح بزيادة الموارد بسرعة أو إزالة الموارد المخصصة بشكل مفرط لإدارة التكاليف.

جميع الأنظمة الرئيسية ضمن بنية الحوسبة الخاصة بالشركة يتم نسخها احتياطيًا بانتظام. تمتلك خدمات تكنولوجيا المعلومات استراتيجية نسخ احتياطي تحدد تكرار النسخ الاحتياطية. يُوصى أيضًا بشدة أن يقوم جميع المستخدمين بحفظ عملهم على محرك الشبكة الخاص بهم؛ حيث يتم نسخ هذا المحرك احتياطيًا وأي فقدان أو تلف للملفات يمكن غالبًا إصلاحه من خلال استعادة الملفات من النسخة الاحتياطية الموجودة.