VECTOR >

Technical and Organizational Measures

[German, Japanese and Korean version below]

This document describes which technical and organizational measures are established to ensure information security and data protection. The aim is to guarantee in particular the confidentiality, integrity and availability of the information processed by the company.

Guideline

The guidelines, in particular the “Process Description Information Security Management” (PD ISM) contains the management’s key messages on information security in the company. All internal and external employees of the Vector Group as well as its suppliers are obligated to comply with the central rules, which apply worldwide.

The level of security of organizational units, processes and IT systems is monitored through periodic audits and ongoing controls. The monitoring of ongoing operations is carried out in coordination with Quality Management. A review of the security policy is carried out at least annually, unless a major change requires an earlier review. This ensures the suitability, appropriateness and effectiveness of the regulations on an ongoing basis.

The Chief Information Security Officer is responsible for the security policy and is tasked with developing, revising and reviewing it.

Organization

Information security roles and responsibilities are defined for Vector's processes. Conflicting roles and responsibilities are segregated in order to reduce the risk of unauthorized or unintended modification or abuse of data.

Data sets and IT systems (assets) relating to personal data and sensitive information are inventoried and maintained. To protect these assets, persons are designated who have responsibility for the life cycle of an asset. The information and data are classified and labelled based on legal requirements, their value, criticality and sensitivity to unauthorized disclosure or modification, using a multi-level classification scheme which categories personal data.

Based on the classification, sensitive IT systems with increased requirements are defined to ensure that information and personal data are protected. Resulting risks are regularly assessed and addressed accordingly.

Other risks arising from planned changes, security incidents or data breaches are systematically assessed and addressed with the required measures. All systems in use are subject to patch management to ensure secure operation in terms of confidentiality, integrity, and availability.

Vector maintains ongoing contact with special stakeholder groups to keep abreast of changes and improvements relating to data protection and information security.

Staff Security

All employees are obligated to maintain confidentiality and to comply with the provisions on information security and data protection set out in their employment contract.

To increase general awareness, training measures are carried out on a regular basis covering various aspects of daily work at Vector (e.g. password security, reporting channels for security incidents). Target groups with specific roles and functions (e.g. IT administrators, information owners) shall receive additional training.

Further regulations on mobile work and the use of mobile devices ensure data protection and information security even in areas that are not under the direct influence of Vector. In this case, access to company resources is only possible via dedicated and encrypted connections.

Physical Security and Business Continuity

All of Vector's buildings and work premises are protected by a multi-tier zone concept to prevent unauthorized access and entry of premises, as well as access to IT systems or documents. Each zone has its own regulations and technical security mechanisms (e.g. locking concept). These security mechanisms shall also be maintained in an emergency until the appropriate recovery measures are taken and a return to the building is possible again.

Vector has contingency plans in place to enable continuity of business operations. To this end, emergency plans shall be regularly reviewed and tested. In this context, backups of central IT systems are a major component of a holistic strategy.

Identity and Access Management

Identity management is an essential element for the correct allocation of access permissions. Vector has opted for a centralized approach that controls both internal and external identities for essential IT systems.

Access is controlled using the centrally managed identities in the individual IT systems with corresponding processes and procedures. In addition to setting up such identities, this also includes reviewing and revoking information access permissions that are no longer required.

IT Security / Cyber Security

The procurement, development and maintenance of IT systems at Vector is based on IT processes, in particular risk-based project and change management.

When changes to operating platforms are made, mission-critical applications shall be reviewed and tested to ensure that there is no negative impact on organizational activities or organizational security.

These changes shall be logged.

The development follows a controlled process for the analysis, development, and maintenance of secure IT systems. Updates are imported and released centrally on a regular basis.

Acceptance test programs and relevant criteria are defined for new IT systems, updates, and new versions. All changes shall be approved by a central change advisory board. Access to production information is managed by identity and access management. As a rule, production data is not used for testing purposes. If necessary, this is evaluated by the CISO and the production data are protected during testing by comparable security mechanisms (e.g. the same permissions as in production, pseudonymization, anonymization).

The security of the networks and the personal data and information stored in network services is also of essential importance. To ensure their protection, organizational measures are in place to manage, control and secure the networks. Data is always transferred via the network using encrypted connections. Data connections from unauthorized networks are prevented. Information services, users and IT systems shall be kept segregated from each other as required. Policies and procedures have been implemented for the transfer of information and data, as well as security agreements concluded for the transfer of information to external parties. Adequate security is provided for electronic messaging through measures protecting messages from unauthorized access or modification in accordance with the classification scheme adopted by the organization.

State-of-the-art cryptographic procedures are used to ensure the technical security of IT systems and networks. These include procedures for encrypting information according to its classification as "data in motion", "data in use" and "data in rest".

Relationships with Suppliers

Vector evaluates suppliers in advance based on standardized criteria and checks their suitability regarding maintaining data and information security. The selection and regular review of suppliers is based on whether they process information requiring protection, provide services or hardware for customer projects which require a high level of protection or if they provide IT services (e.g. cloud, SaaS, managed services) for Vector.

The processing, correction and in particular the erasure of the data is carried out in accordance with the

orders and individual instructions of the data controller and, where applicable, in accordance with the contractual or statutory retention periods. To protect data and information, Vector enters into confidentiality agreements, non-disclosure agreements or commissioned data processing agreements as required.

Suppliers are required to implement technical and organizational measures to ensure security. The quality of service, which also includes security aspects (availability), is regulated by SLAs.

To ensure supply chain security, suppliers may only use other suppliers with our consent. Regular supplier audits ensure that the agreed level is maintained.

After termination of the supplier relationship, the supplier is obligated to destroy the data and information received from us. In addition, the confidentiality obligation applies indefinitely.

Compliance

Vector has identified, documented and keeps up to date the relevant legal, regulatory, self-imposed and contractual requirements and our company's approach to complying with them. Appropriate procedures have also been implemented to ensure compliance with legal, regulatory and contractual requirements relating to intellectual property rights and the use of proprietary software products. In accordance with legal, regulatory, contractual and business requirements, records and personal information are protected as necessary.

To ensure the protection of our information and data, an independent review of our level of information security and data protection, our security and data protection policies, as well as of our compliance with technical requirements is carried out on a regular basis.

VECTOR >

Technische und Organisatorische Maßnahmen

[German version]

Im Folgenden wird beschrieben, welche technischen und organisatorischen Maßnahmen zur Gewährleistung von Informationssicherheit und Datenschutz festgelegt werden. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Unternehmen verarbeiteten Informationen.

Leitlinie

Die Leitlinien, insbesondere die „Prozessbeschreibung Information Security Management“ (PD ISM) beinhaltet die Leitaussagen der Geschäftsleitung zur Informationssicherheit im Unternehmen. Alle internen und externen Mitarbeiterinnen und Mitarbeiter der Vector Gruppe sowie Lieferanten sind verpflichtet, die zentralen Regelungen zu berücksichtigen. Die Regelungen gelten weltweit.

Das Sicherheitsniveau der Organisationseinheiten, Prozesse und IT-Systeme wird durch periodisch wiederkehrende Prüfungen sowie kontinuierlichen Kontrollen überwacht. Die Überwachungen des laufenden Betriebs erfolgten in Abstimmung mit dem Qualitätsmanagement. Ein Review der Sicherheitspolitik erfolgt zumindest jährlich, soweit nicht eine wesentliche Änderung dies früher erfordert. Hierdurch werden laufend die Eignung, Angemessenheit und Wirksamkeit der Regelungen sichergestellt.

Der Informationssicherheitsbeauftragte (Chief Information Security Officer) ist der Verantwortliche für die Sicherheitspolitik und hat die Verantwortung, diese zu entwickeln, zu überarbeiten und zu prüfen.

Organisation

Informationssicherheitsrollen und -verantwortlichkeiten sind in den Prozessen von Vector definiert. Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um das Risiko zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Informationen zu reduzieren.

Werte und IT-Systeme (Assets), die mit personenbezogenen Daten und schützenswerten Informationen in Zusammenhang stehen, werden inventarisiert und gepflegt. Zum Schutz dieser Werte sind Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind. Die Informationen und Daten werden anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert und gekennzeichnet. Dazu wird ein mehrstufiges Klassifizierungsschema genutzt, in welchem Kategorien von personenbezogenen Daten berücksichtigt werden.

Auf Grundlage der Klassifizierung werden sensible IT-Systeme mit erhöhten Anforderungen qualifiziert, um den Schutz von Informationen und personenbezogenen Daten zu gewährleisten. Daraus entstehende Risiken werden regelmäßig bewertet und entsprechend behandelt.

Weitere Risiken, die sich aus geplanten Änderungen, Sicherheitsvorfällen oder Datenpannen ergeben, werden systematisch bewertet und mit erforderlichen Maßnahmen behandelt. Für alle eingesetzten Systeme wird durch das Patchmanagement sichergestellt, dass ein sicherer Betrieb im Sinne der Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet werden kann.

Vector pflegt laufenden Kontakt zu speziellen Interessensgruppen, um über Änderungen und Verbesserungen im Bereich Datenschutz und Informationssicherheit informiert zu sein.

Personalsicherheit

Alle Mitarbeiterinnen und Mitarbeiter sind zur Geheimhaltung und zur Einhaltung der Regelungen aus der Informationssicherheit und dem Datenschutz in ihrem Arbeitsvertrag verpflichtet.

Um die allgemeine Sensibilisierung zu erhöhen, werden regelmäßige Schulungen durchgeführt, die verschiedene Aspekte der täglichen Arbeit bei Vector umfassen (z.B. Passwortsicherheit, Meldewege bei Sicherheitsvorfällen). Zielgruppen mit spezifischen Rollen und Funktionen (z.B. IT-Administratoren, Information Owner) werden zusätzlich trainiert.

Durch weiterführende Regelungen zur mobilen Arbeit sowie der Nutzung von mobilen Endgeräten, werden Datenschutz und die Informationssicherheit auch in Bereichen sichergestellt, die nicht unter dem direkten Einfluss von Vector liegen. Der Zugriff auf Unternehmensressourcen ist in diesem Falle nur über dedizierte und verschlüsselte Verbindungen möglich.

Physische Sicherheit und Business Continuity

Sämtliche Gebäude und Arbeitsräumlichkeiten von Vector sind durch ein mehrstufiges Zonenkonzept geschützt, um den unberechtigten Zugang, Zutritt und Zugriff auf IT-Systeme oder Unterlagen zu verhindern. Jede Zone verfügt über eigene Regelungen und technische Schutzmechanismen (z.B. Schließkonzept). Diese Schutzmechanismen werden auch im Notfall aufrechterhalten, bis die entsprechenden Wiederherstellungsmaßnahmen ergriffen sind und eine Rückkehr ins Gebäude wieder möglich ist.

Vector verfügt über Notfallpläne, die eine Fortführung des Geschäftsbetriebs ermöglichen. Dazu werden Notfallpläne regelmäßig geprüft und getestet. Die Nutzung von Backups von zentralen IT-Systemen ist dabei ein wesentlicher Baustein zu einer ganzheitlichen Strategie.

Identitäts- und Berechtigungsmanagement

Die Verwaltung von Identitäten ist ein wesentliches Element für die korrekte Zuordnung von Berechtigungen. Vector hat sich hier für einen zentralen Ansatz entschieden, der sowohl interne als auch externe Identitäten für wesentliche IT-Systeme steuert.

Der Zugriff wird unter Nutzung der zentral bereitgestellten Identitäten in den einzelnen IT-Systemen mit entsprechenden Prozessen und Verfahren gesteuert. Dies beinhaltet neben der Einrichtung, ebenso die Überprüfung und den Entzug von nicht mehr erforderlichen Berechtigungen auf Informationen.

IT-Sicherheit / Cyber Security

Die Anschaffung, Entwicklung und Wartung von IT-Systemen beruht bei Vector auf IT-Prozessen, insbesondere einem risikoorientierten Projekt- und Changemanagement.

Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder die Organisationssicherheit gibt. Diese Änderungen werden protokolliert.

Die Entwicklung folgt dabei einem gesteuerten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT- Systeme. Updates werden regelmäßig zentral eingespielt und freigegeben.

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt. Sämtliche Änderungen werden durch ein zentrales Gremium freigegeben. Zugriffe auf produktive Informationen werden durch das Identity- und Access Management verwaltet. Produktivdaten werden in der Regel nicht zu Testzwecken genutzt. Sofern dies erforderlich ist, wird dies durch den CISO bewertet und durch vergleichbare Schutzmechanismen (z.B. gleiche Berechtigungen wie in Produktion, Pseudonymisierung, Anonymisierung) geschützt.

Darüber hinaus ist die Sicherheit der Netzwerke und in Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen unumgänglich. Daher werden die Netzwerke durch organisatorische Maßnahmen verwaltet, gesteuert und gesichert. Der Transport von Daten findet grundsätzlich per Netzwerk über verschlüsselte Verbindungen statt. Der Aufbau von Datenverbindungen aus nicht zugelassenen Netzwerken wird unterbunden. Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt gehalten. Es wurden Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen implementiert. Elektronische Nachrichtenübermittlung wird angemessen geschützt, indem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff oder vor Veränderung getroffen wurden, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Für die technische Sicherheit von IT-Systemen und Netzwerken werden kryptografische Verfahren nach dem Stand der Technik eingesetzt. Diese umfassen Verfahren zur Verschlüsselung von Informationen entsprechend ihrer Klassifikation aus den Perspektiven „Data in Motion“, „Data in Use“ und „Data in Rest“.

Lieferantenbeziehungen

Vector wählt Lieferanten im Vorfeld nach standardisierten Kriterien aus und überprüf die Eignung hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes. Die Auswahl und die regelmäßige Überprüfung von Lieferanten wird auf der Grundlage bewertet, ob diese schützenswerten Informationen verarbeiten, Dienstleistungen oder Hardware für Kundenprojekte mit sehr hohem Schutzbedarf liefern oder IT-Services (z.B. Cloud, SaaS, Managed Services) für Vector bereitstellen.

Die Verarbeitung, Berichtigung und insbesondere Löschung der Daten erfolgt gemäß Auftrag und Einzelweisungen des Verantwortlichen sowie ggf. entsprechend den vertraglichen oder gesetzlichen Aufbewahrungsfristen. Um Daten und Informationen zu schützen, schließt Vector bedarfsgerechte Vertraulichkeits-, Geheimhaltungsvereinbarungen oder Auftragsverarbeitungsvereinbarungen ab.

Die Lieferanten werden verpflichtet, technisch-organisatorische Maßnahmen zu treffen, um die Sicherheit zu gewährleisten. Die Servicequalität, welche auch Aspekte der Sicherheit umfasst (Verfügbarkeit), wird durch SLAs vereinbart.

Lieferanten dürfen weitere Lieferanten lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten. Regelmäßige Lieferantenaudits stellen sicher, dass das vereinbarte Niveau aufrechterhalten werden kann.

Nach Beendigung des Lieferantenverhältnisses sind diese verpflichtet, die von uns erhaltenen Daten und Informationen zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht unbegrenzt.

Compliance

Vector hat die relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und auf dem neuesten Stand gehalten. Auch wurden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist. Entsprechend der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen werden Aufzeichnungen und personenbezogene Informationen bedarfsgerecht geschützt.

Um den Schutz unserer Informationen und Daten sicher zu stellen, erfolgt regelmäßig eine unabhängige Überprüfung unseres Informationssicherheits- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

VECTOR >

技術的安全管理措置および組織的安全管理措置

[Japanese version]

本書では、情報セキュリティとデータ保護を確保するためにどのような技術的安全管理措置および組織的安全管理措置が定められているかを説明しています。その目的は、特にベクターが処理する情報の機密性、完全性および可用性を保証することにあります。

ガイドライン

ガイドライン、特に「Process Description Information Security Management」（PD ISM）には、社内の情報セキュリティに関する経営陣の重要メッセージが記載されています。ベクターグループの従業員および派遣社員の全員とベクターのサプライヤーは、世界全域で適用される主要ルールを遵守する義務を負います。

組織単位、プロセスおよびITシステムのセキュリティレベルは、定期監査と継続的管理により監視されています。日常業務の監視は、品質管理業務と連携のうえ実施されています。セキュリティポリシーについては、重要な変更によりさらに早期の精査が必要とならない限り、年1回以上の頻度で精査されます。これにより、規則の適合性、適切性、有効性が常に確保されます。

最高情報セキュリティ責任者（CISO）は、セキュリティポリシーに責任を負い、その策定、改訂および精査を担います。

組織

ベクターのプロセスに関して、情報セキュリティの役割と責任が定義されています。役割と責任に相反が生じた場合、データの不正もしくは意図しない改変または悪用のリスクを軽減するために、その役割と責任は分離されます。

個人データと機微（センシティブ）情報に関係するデータセットおよびITシステム（資産）は、棚卸され管理されています。これらの資産を保護するために、資産のライフサイクル責任者が選任されています。情報とデータは、個人データを分類する多層分類法を用いて、法的要件、それらの価値、重大性、不正な開示もしくは改変に対する脆弱性に基づき区分され、表示されています。

こうした区分に基づき、要件数が多く機密性の高いITシステムは、情報と個人データが確実に保護されるよう定義されます。これにより、そうしたシステムに伴うリスクが定期的に評価・対処されます。

計画的な変更、セキュリティ事故またはデータ侵害により生じるその他のリスクは、所要の措置により体系的に評価・対処されます。使用中のシステムはすべて、機密性・完全性・可用性の観点から安全な運用を図るためにパッチ管理の対象となっています。

ベクターは、特別な利害関係グループと常に連絡体制を維持し、データ保護と情報セキュリティに関する変更や改善があった場合には遅滞なく通知できるようにしています。

人的安全管理措置

従業者全員が、秘密を保持し、各自の雇用契約に定める情報セキュリティとデータ保護に関する規定を遵守する義務を負います。

一般的な意識向上を図るために、ベクターにおける日常業務のさまざまな側面（たとえば、パスワードのセキュリティ、セキュリティ事故の報告経路）を対象とした研修活動が定期的に実施されています。特定の役割と職務を担う対象グループ（たとえば、IT管理者、情報所有者）は、さらに詳しい研修を受けるものとします。

モバイルワークとモバイル機器の使用に関してさらに規則を策定することにより、ベクターの直接的な影響下にない場所においてもデータ保護と情報セキュリティの徹底を図っています。こうした場合、会社資源へのアクセスは専用の暗号化された回線を使用する場合に限定されます。

物理的セキュリティと業務継続性

ベクターの建物と業務施設はすべて、施設への不正なアクセスと立ち入りのほか、ITシステムまたは文書へのアクセスを防止する多層ゾーンの概念により保護されています。ゾーンごとに、独自の規則と技術的セキュリティメカニズム（たとえば、ロッキングの概念）が実施されています。緊急事態発生時にも、適切な回復措置が講じられ、建物の使用が再開されるまで、こうしたセキュリティメカニズムが維持されるものとします。

ベクターは、業務を継続できるよう緊急時対応計画を用意しています。そうした事態に備えて、緊急時を想定した計画の定期的な精査とテストを実施するものとします。こうした状況では、基幹ITシステムのバックアップが全体的戦略の重要な要素となります。

ID管理およびアクセス管理

ID管理は、アクセス許可を正確に割り当てるために不可欠な要素です。ベクターは、重要ITシステムの社内外のID情報について一元管理方式を選択しています。

アクセス管理は、対応するプロセスや手順と併せて、個々のITシステム上で一元的に管理されているID情報を用いて行われています。これには、こうしたID情報の設定のほかに、必要でなくなった情報アクセス許可の精査と削除も含まれます。

ITセキュリティ/サイバーセキュリティ

ベクターにおけるITシステムの調達・開発・保守は、ITプロセス、特にリスクベースのプロジェクトと変更の管理を基本としています。

業務プラットフォームが変更された場合、ミッションクリティカルなアプリケーションは、組織の活動または組織のセキュリティへの負の影響がないことを確かめるために精査・テストされるものとします。

業務プラットフォームの変更は記録されるものとします。

開発は、セキュアなITシステムの解析・開発・保守用に管理されたプロセスに従って行われます。更新は、定期的且つ一元的に取り込まれ公開されます。

新しいITシステム、更新および新バージョンについて、受入れテストプログラムと関連基準が定義されます。変更はすべて、change advisory boardの承認を受けるものとします。実稼働情報へのアクセス管理はID管理とアクセス管理により行われます。

原則として、実稼働データはテスト目的で使用されません。必要な場合、CISOの評価を受け、テスト中においても同等のセキュリティメカニズム（たとえば、実稼働中、仮名化中、匿名化中のものと同じ許可）により実稼働データは保護されます。

ネットワークならびにネットワーク・サービスに保管された個人データおよび個人情報のセキュリティもまた、非常に重要です。それらの保護を徹底するために、ネットワークを管理・統制し、安全に保護する組織的安全管理措置が実施されています。データの移転は常に、暗号化された接続を用いてネットワーク経由で行われます。認証されていないネットワークからのデータ接続は、未然に防止されます。情報サービス、ユーザーおよびITシステムは、必要に応じて、互いに隔離された状態に置かれるものとします。情報とデータの移転のほか、外部者への情報を移転するために締結されるセキュリティ契約について、ポリシーと手順が実施されています。電子メッセージの送受信に際しては、組織が採用している分類体系に従い、認証されていないアクセスまたは改変からメッセージを保護する対策により十分なセキュリティが提供されています。

ITシステムとネットワークの技術的セキュリティを確保するために、最新の暗号化手順が用いられています。これには、情報が「移転中のデータ（data in motion）」「使用中のデータ（data in use）」「保存のデータ（data in rest）」のいずれに分類されるかにより暗号化する手順も含まれています。

サプライヤーとの関係

ベクターは、標準化された基準に基づきサプライヤーを事前に評価し、データと情報のセキュリティ確保に関する適合性を確認します。サプライヤーの選定と定期精査の基準となるのは、サプライヤーが、保護を必要とする情報を処理しているか、高度な保護を必要とする顧客のプロジェクトにサービスまたはハードウェアを提供しているか、またはベクターのためにITサービス（たとえば、クラウド、SaaS、マネージド・サービス）を

提供しているかです。

データの処理・修正、とりわけデータの消去は、データ管理者からの指図や個別指示に従い、さらに該当する場合には、契約上または制定法上の保管期間に従い、実行されます。データと情報を保護するために、ベクターは、必要に応じて、秘密保持契約（NDA）またはデータ処理業務委託契約を締結します。

サプライヤーは、セキュリティを確保するために技術的安全管理措置と組織的安全管理措置を講じることを要求されます。サービスの質（セキュリティに関する側面（可用性）も含まれます）は、サービス・レベル契約（SLA）に定められています。

サプライチェーンのセキュリティを確保するために、サプライヤーは、ベクターの同意を得た場合に限り、別のサプライヤーに業務の一部を委託することができます。サプライヤーの定期監査により、合意されたレベルが維持されるようにします。

サプライヤー関係の終了後も、サプライヤーは、ベクターから受領したデータと情報を破棄する義務を負います。そのうえで、秘密保持義務が無期限に適用されます。

法令遵守

ベクターは、関連法令・規則上、自主規制上および契約上の要件とベクターによるそれらの遵守方法を確認・記録しており、それらに関する情報を常に最新化しています。知的財産権と独自のソフトウェア製品の使用に関する法令・規則上および契約上の要件の遵守を徹底するために、適切な手順も実施しています。記録と個人情報は、必要に応じて、法令・規則上、契約上および業務上の要件に従い、保護されています。

ベクターの情報とデータの保護を徹底するために、ベクターの情報セキュリティとデータ保護のレベル、ベクターのセキュリティとデータ保護に関するポリシー、さらにはベクターによる技術要件の適合状況について、定期的に独自の精査を実施しています。

VECTOR >

기술적, 관리적 및 물리적 조치

[Korean version]

이 문서는 정보보호와 데이터 보호를 보장하기 위해 마련된 기술적, 관리적 및 물리적 관리 조치를 설명합니다. 본 문서의 목적은 특히 당사가 처리하는 정보의 기밀성, 무결성 및 가용성을 보장하는 데 있습니다.

가이드라인

가이드라인, 특히 “Process Description Information Security Management” (PD ISM)에는 회사의 정보 보안에 관한 경영진의 핵심 메시지가 포함되어 있습니다. Vector 그룹의 모든 내부 및 파견 직원과 공급업체는 전 세계적으로 적용되는 주요 규칙을 준수해야 합니다.

조직 단위, 프로세스 및 IT 시스템의 보안 수준은 정기적인 감사와 지속적인 관리를 통해 모니터링됩니다. 일상 운영의 모니터링은 품질 관리 부서와 협력하여 수행됩니다. 보안 정책은 최소 연 1회 검토되며, 주요 변경 사항이 있을 경우 더 일찍 검토됩니다. 이를 통해 규정의 적합성, 적절성 및 효과성이 지속적으로 보장됩니다.

최고 정보 보안 책임자(CISO)는 보안 정책의 책임을 지며, 정책의 수립, 개정 및 검토를 담당합니다.

조직

정보 보안 역할과 책임은 Vector의 프로세스를 위해 정의되어 있습니다. 그리고 데이터의 무단 또는 의도치 않은 변경이나 오용의 위험을 줄이기 위해 상충되는 역할과 책임은 분리됩니다.

개인 데이터 및 민감한 정보와 관련된 데이터 세트와 IT 시스템(자산)은 목록화되고 유지 관리됩니다. 이러한 자산을 보호하기 위해 자산의 수명주기(Life cycle)에 대한 책임을 지는 담당자가 지정됩니다. 정보와 데이터는 법적 요구사항, 그 가치, 중요성, 무단 공개 또는 변경에 대한 민감도를 기준으로, 개인정보를 분류하는 다단계 분류 체계를 사용하여 분류 및 라벨링됩니다.

분류 체계에 따라, 정보와 개인정보가 보호되도록 요구사항이 강화된 민감한 IT 시스템을 정의합니다. 이에 따른 위험은 정기적으로 평가되고 적절히 대응됩니다.

계획된 변경, 보안 사고 또는 데이터 침해로 인한 기타 위험은 체계적으로 평가되고 필요한 조치가 취해집니다. 모든 시스템은 기밀성, 무결성, 가용성을 보장하기 위해 패치 관리(Patch management) 대상이 됩니다.

Vector는 데이터 보호 및 정보 보안 관련 변경 사항과 개선 사항을 신속히 파악하기 위해 특정 이해관계자 그룹과 지속적으로 연락 체계를 유지합니다.

인적 보안

모든 직원은 비밀 유지 의무를 지며, 고용 계약에 명시된 정보 보안 및 데이터 보호 규정을 준수해야 합니다.

일반적인 보안 인식을 높이기 위해, Vector의 일상 업무와 관련된 다양한 측면(예: 비밀번호 보안, 보안 사고 보고 경로)을 다루는 교육이 정기적으로 실시됩니다. 특정 역할과 기능권한을 가진 대상 그룹(예: IT 관리자, 정보 소유자)은 추가 교육을 받아야 합니다.

모바일 근무 및 모바일 기기 사용에 관한 추가 규정은 Vector의 직접적인 관리 범위를 넘어선 영역에서도 데이터

보호와 정보 보안을 효과적으로 보장합니다. 이 경우, 회사 리소스 접근은 전용 암호화 연결을 통해서만 가능합니다.

물리적 보안 및 비즈니스 연속성

Vector의 모든 건물과 작업장은 무단 접근 및 출입뿐만 아니라 IT 시스템이나 문서에 대한 접근을 방지하기 위해 다단계 구역 개념(Multi-tier Zone Concept)으로 보호됩니다. 각 구역은 자체 규정과 기술적 보안 메커니즘(예: 잠금 시스템)을 갖추고 있습니다. 비상 상황에서도 이러한 보안 메커니즘이 유지되며, 적절한 복구 조치가 완료되고 건물로의 복귀가 가능해질 때까지 적용됩니다.

Vector는 비즈니스 운영의 연속성을 보장하기 위해 비상 대응 계획을 마련하고 있습니다. 이를 위해 비상 계획은 정기적으로 검토되고 테스트됩니다. 이와 관련하여, 중앙 IT 시스템의 백업은 전체 전략의 핵심 요소입니다.

ID 및 접근 관리

ID 관리(Identity Management)는 접근 권한을 올바르게 부여하기 위한 필수 요소입니다. Vector는 핵심 IT 시스템에 대한 내부 및 외부 ID를 모두 제어하는 중앙 집중식 방식을 채택했습니다.

접근은 각 IT 시스템에서 중앙에서 관리되는 ID와 해당 프로세스 및 절차를 사용하여 제어됩니다. ID를 설정하는 것뿐만 아니라, 더 이상 필요하지 않은 정보 접근 권한을 검토하고 철회하는 작업도 포함됩니다.

IT 보안 / 사이버 보안

Vector에서 IT 시스템의 조달, 개발 및 유지보수는 IT 프로세스, 특히 위험 기반 프로젝트 및 변경 관리(Risk-based Project and Change Management)에 기반합니다.

운영 플랫폼 변경 시, 핵심 애플리케이션은 조직의 활동이나 보안에 부정적인 영향이 없도록 검토 및 테스트됩니다.

이러한 변경 사항은 모두 기록됩니다.

개발은 보안 IT 시스템의 분석, 개발 및 유지보수를 위한 관리 프로세스를 따릅니다. 업데이트는 중앙에서 정기적으로 수집되어 배포됩니다.

새로운 IT 시스템, 업데이트 및 신규 버전에 대한 수용 테스트 프로그램과 관련 기준이 정의되어 있습니다. 모든 변경 사항은 중앙 위원회(Central Change Advisory Board)의 승인을 받아야 합니다. 운영 정보에 대한 접근은 ID 및 접근 관리로 통제됩니다. 원칙적으로 운영 데이터는 테스트 목적으로 사용되지 않습니다. 필요한 경우, CISO의 평가를 거쳐 운영 데이터는 테스트 중에도 동등한 보안 메커니즘 (예: 운영 데이터와 같은 권한 관리, 가명화, 익명화) 으로 보호됩니다.

네트워크 및 네트워크 서비스에 저장되는 개인정보와 정보의 보안은 본질적으로 매우 중요한 사항입니다. 이를 위해 네트워크를 관리, 통제 및 보호하는 조직적 조치가 마련되어 있습니다. 데이터는 항상 암호화된 연결을 통해 네트워크로 전송됩니다. 인가되지 않은 네트워크로부터의 데이터 연결은 차단됩니다. 정보 서비스, 사용자 및 IT 시스템은 필요에 따라 서로 분리됩니다. 정보 및 데이터 전송을 위한 정책과 절차가 확립되어있으며, 외부로의 정보 전송을 위한 보안 계약도 체결되었습니다. 전자 메시지 전송 시에는 조직에서 채택한 분류 체계에 따라 무단 접근이나 변경으로부터 메시지를 보호하는 조치를 통해 적절한 보안이 제공됩니다.

IT 시스템과 네트워크의 기술적 보안을 보장하기 위해 최신 암호화 절차가 적용됩니다. 여기에는 ‘전송 중 데이터(Data in Motion)’, ‘사용 중 데이터(Data in Use)’, ‘저장 데이터(Data at Rest)’로 분류된 정보에

대한 암호화 절차가 포함됩니다.

공급업체 관계

Vector는 표준화된 기준에 따라 사전에 공급업체를 평가하고, 공급업체의 데이터 및 정보 보안 유지 적합성을 확인합니다. 공급업체의 선정 및 정기 검토는 해당 업체가 보호가 필요한 정보를 처리하는지, 높은 수준의 보호가 요구되는 고객 프로젝트에 서비스 또는 하드웨어를 제공하는지, 또는 Vector를 위해 IT 서비스(예: 클라우드, SaaS, 관리형 서비스)를 제공하는지 여부를 기준으로 합니다.

데이터의 처리, 정정 및 특히 삭제는 데이터 관리자의 지시 및 개별 지침에 따라, 그리고 해당되는 경우 계약상 또는 법정 보존 기간에 따라 수행됩니다. 데이터와 정보를 보호하기 위해, Vector는 필요 시 비밀유지계약(NDA), 비공개계약 또는 위탁 데이터 처리 계약을 체결합니다.

공급업체는 보안을 보장하기 위해 기술적· 조직적 조치를 시행해야 합니다. 서비스 품질(가용성 등 보안 측면 포함)은 SLA에 의해 규율됩니다.

공급망 보안을 보장하기 위해, 공급업체는 당사의 동의 없이 제3의 공급업체를 사용할 수 없습니다. 정기적인 공급업체 감사는 합의된 수준이 유지되도록 합니다.

공급업체 관계 종료 후, 공급업체는 당사로부터 받은 데이터와 정보를 파기해야 하며, 비밀유지 의무는 무기한 적용됩니다.

규제 준수 (Compliance)

Vector는 관련 법령, 규제, 자체 기준 및 계약상 요구사항과 이에 대한 당사의 준수 방안을 식별하고 문서화하며 최신 상태로 유지합니다. 또한 지식재산권 및 상용 소프트웨어 제품의 사용과 관련된 법령·규제·계약상 요구사항을 준수하기 위한 적절한 절차를 수립하고 이행합니다. 법령, 규제, 계약 및 사업상 요구사항에 따라 기록과 개인정보를 필요한 수준으로 보호합니다.

Vector의 정보와 데이터를 철저히 보호하기 위하여, 당사의 정보보호 및 데이터 보호 수준, 보안 및 데이터 보호에 관한 정책, 그리고 기술적 요구사항 준수 여부에 대한 독립적인 정기 검토를 실시합니다.