ZUSAMMENFASSUNG

SUMÁRIO

1. EINFÜHRUNG

Das Hauptziel dieser Informationssicherheitspolitik für Partner ist es, ein effektives Programm zum Schutz von Informationswerten zu leiten, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten, das die Grundlage für die Festlegung von Informationssicherheitsstandards und -verfahren in der WEG-Gruppe bildet.

2. SCOPE

Alle Partner (jede Person, die mit der WEG-Gruppe eine rechtliche Beziehung als Lieferant von Produkten, Lizenzen oder Dienstleistungen unterhält) müssen die hier definierten Anforderungen an die Informationssicherheit einhalten.
Die Einhaltung der festgelegten Richtlinien ist eine wesentliche Voraussetzung für eine wirksame Partnerschaftsbeziehung und die Erreichung eines angemessenen Datenschutzniveaus.
Die hierin festgelegten Richtlinien und Anforderungen gelten für alle Partner, die Zugang zu den Daten, Informationen und Systemen der WEG-Gruppe haben. Die Partner sind für sich selbst und ihre Mitarbeiter, Lieferanten und Dienstleister verantwortlich.

3. DEFINITIONEN

- **DPIA:** ist die Abkürzung für Data Protection Impact Assessment (Datenschutz-Folgenabschätzung), die im brasilianischen Allgemeinen Datenschutzgesetz (LGPD) für Personal Data Protection Impact Report (RIPD) steht. Dieser Prozess identifiziert, bewertet und mindert die Risiken für den Datenschutz bei Datenprojekten, bevor diese umgesetzt werden. Es handelt sich um eine gesetzliche und obligatorische Verantwortung, wenn die Datenverarbeitung die Rechte und Freiheiten der betroffenen Personen gefährden kann.
- **Opt-in:** Ein englischer Begriff, der die Zustimmung eines Benutzers bedeutet, Informationen von einem Unternehmen zu erhalten.
- **Opt-out:** Ein Begriff aus dem Englischen, der so viel bedeutet wie „sich entscheiden, auszusteigen“. Es handelt sich um eine Bewegung, bei der der Einzelne die Autonomie hat, nicht mehr Teil von etwas zu sein, das ihm eingegeben wurde.
- **Trennung der Zuständigkeiten (SOD):** SOD ist die Abkürzung für Segregation of Duties (Aufgabentrennung), ein Prinzip der internen Kontrolle, das darauf abzielt, Risiken wie Betrug, Fehler und Cyberangriffe in Organisationen zu vermeiden. Die Aufgabentrennung basiert auf der Delegation von Aufgaben zwischen verschiedenen Personen oder Gruppen, um zu verhindern, dass ein und dieselbe Person die volle Kontrolle über Systeme, Prozesse oder vertrauliche Aktivitäten hat.
- **Politik der geringsten Privilegien:** Dies ist ein Cybersicherheitskonzept, das darin besteht, Benutzern nur die geringsten Privilegien zu gewähren, die für die Erfüllung ihrer Aufgaben erforderlich sind.
- **Runbooks:** Detaillierte Leitfäden, die die Verfahren und Prozesse einer Organisation beschreiben, um sicherzustellen, dass die Aktivitäten einheitlich, sicher und effizient durchgeführt werden.
- **Härtung:** Ein Prozess, der darauf abzielt, die Sicherheit von Systemen, Netzwerken, Software, Hardware, Firmware und IT-Infrastrukturen zu stärken und sie damit widerstandsfähiger gegen Cyberangriffe zu machen.
- **Sicherheits-Patches:** korrigierende Updates, die darauf abzielen, Schwachstellen, Fehler und Bugs in Software und Plattformen zu beheben. Das Wort „Patch“ ist ein englischer Begriff und bedeutet „Flicken“ oder „Flicken“.

- **OWASP:** Open Worldwide Application Security Project (OWASP) ist eine internationale Non-Profit-Organisation, die sich für die Verbesserung der Sicherheit von Web- und mobilen Anwendungen einsetzt. OWASP ist eine der führenden Initiativen zur Bekämpfung der Internetkriminalität.
- **Privacy und Security by Design:** Konzepte, die sich proaktiv auf Datenschutz und Systemsicherheit beziehen, und zwar bereits bei der Konzeption eines Projekts oder einer Dienstleistung.
- **Phishing:** eine Art von Cyberangriff, der darauf abzielt, persönliche Informationen zu stehlen oder auf Online-Konten zuzugreifen. Betrüger verwenden betrügerische Nachrichten, die legitim erscheinen, um Opfer dazu zu bringen, sensible Daten preiszugeben.
- **Ethisches Hacken:** Ethical Hacking oder ethisches Hacken ist eine digitale Sicherheitspraxis, die darin besteht, einen Cyberangriff zu simulieren, um Schwachstellen in Systemen, Netzwerken oder Anwendungen zu identifizieren und zu beheben.
- **Penetrationstests:** Penetrationstests (oder Pentesting) sind autorisierte, simulierte Angriffe, die Unternehmen auf ihre eigenen Computersysteme oder Netzwerke durchführen, um deren Sicherheit zu bewerten. Ziel ist es, Schwachstellen mit denselben Tools, Techniken und Prozessen aufzudecken, die auch von Hackern verwendet werden. Indem sie Schwachstellen in der Cybersicherheit aufdecken, tragen Pen-Tests dazu bei, die Risiken bösartiger Cyberangriffe zu verringern.

4. VERANTWORTLICHKEITEN

4.1. Bereich Lieferantendienstleistungen (Contracting)

- Bei der Einstellung von Partnern (einschließlich Mitarbeitern, Lieferanten und Dienstleistern, die mit dem Partner verbunden sind), die Zugang zum internen Netz, zu Systemen, Informationen oder Daten der WEG-Gruppe benötigen, muss der vertragschließende Bereich sicherstellen, dass alle Beteiligten von dieser Informationssicherheitspolitik Kenntnis haben.
- Der vertragsschließende Bereich muss sicherstellen, dass die Verträge mit den Partnern spezifische Klauseln zur Informationssicherheit und zum Datenschutz enthalten, die auch ausdrücklich auf diese Informationssicherheitspolitik verweisen.

4.2. Partners

- Es liegt in der Verantwortung der Partner, die in dieser Informationssicherheitspolitik dargelegten Richtlinien zu beachten und zu befolgen; und
- Die durchgeführten Aktivitäten müssen mit der geltenden Gesetzgebung und der Standardisierung der Aufsichtsbehörden und Einrichtungen in Bezug auf die Informationssicherheit, die für den Vertragsgegenstand gelten, übereinstimmen.

5. LEITFADEN

5.1. Allgemein

Die Partner, unabhängig davon, ob es sich um Anbieter von Produkten, Lizenzen oder Dienstleistungen handelt, müssen sich verpflichten, die folgenden Punkte vollständig einzuhalten:

- Schutz der Informationen vor unbefugtem Zugriff, Veränderung, Zerstörung oder Offenlegung unter Wahrung der Vertraulichkeit;
- Sicherstellen, dass die ihnen zur Verfügung gestellten Ressourcen nur für die von der WEG-Gruppe genehmigten Zwecke verwendet werden;
- Sicherstellung eines angemessenen Schutzes der Systeme und Informationen, für die er verantwortlich ist, gemäß den Standards der WEG-Gruppe;
- Sicherstellung der Kontinuität der Verarbeitung kritischer Geschäftsinformationen;
- Einhaltung der Gesetze und Normen, die Aspekte des geistigen Eigentums regeln;
- Implementierung und Aufrechterhaltung von Informationssicherheitskontrollen in Übereinstimmung mit den besten Marktpraktiken und den geltenden Vorschriften;
- Unverzügliche Meldung an die WEG-Gruppe bei Verstößen gegen die Informationssicherheitspolitik für Partner durch sie selbst oder durch andere Personen, unabhängig davon, ob sie mit dem Partner verbunden sind oder nicht.
- Die Allgemeinen Bedingungen der WEG-Gruppe für den Einkauf von Waren, Materialien und/oder Dienstleistungen („AGB“) - abrufbar unter: https://www.weg.net/ -> Dies ist WEG -> ALLGEMEINE EINKAUFSBEDINGUNGEN FÜR LIEFERANTEN - und den Ethikkodex der WEG-Gruppe für Lieferanten („Ethikkodex“) - abrufbar unter: https://www.weg.net/ -> Dies ist WEG -> ETHIKKODES FÜR LIEFERANTEN - einzuhalten. Der Partner muss die auf ihn anwendbaren Parameter für den Datenschutz und den Schutz der Privatsphäre, die in den geltenden Rechtsvorschriften festgelegt sind, strikt einhalten und die besten Marktpraktiken zu diesem Thema befolgen.
- Partner, die im Auftrag der WEG-Gruppe kritische Tätigkeiten ausführen, müssen sich einem Bewertungsverfahren für die Informationssicherheit (IS") unterziehen. Im Rahmen des IS-Bewertungsprozesses wird in der Phase der Lieferantenqualifizierung und der Vertragsverhandlungen eine IS-Selbstbewertung durchgeführt. Je nach dem Ergebnis der Selbstbewertung kann die WEG-Gruppe zusätzliche Verfahren verlangen, um zu überprüfen, ob der Partner die in dieser Informationssicherheitspolitik für Partner festgelegten IS-Parameter einhält.

6. ANFORDERUNGEN AN DIE INFORMATIONSSICHERHEIT

6.1. VERHALTEN DER PARTNER IN DER WEG GROUP-UMGEBUNG

6.1.1. Logischer Zugang und akzeptable Nutzung

- Für Partner, die aus der Ferne auf die Umgebung der WEG-Gruppe zugreifen müssen, muss der für den Vertrag verantwortliche WEG-Verwalter den Zugang über einen einzigen und individuellen Benutzer gewähren, mit dem sie nur Zugang zu den Arbeitsressourcen und Umgebungen haben, die für die Erfüllung ihrer Aufgaben erforderlich sind;
- Die Computer der Partner dürfen nicht ohne vorherige Genehmigung des für die Informationssicherheit zuständigen Bereichs an das interne Netz der WEG-Gruppe angeschlossen werden; die Software der Geräte der Partner muss ordnungsgemäß lizenziert sein;
- Es ist verboten, auf Inhalte zuzugreifen, sie herunterzuladen oder zu verbreiten, die das Urheberrecht oder das Eigentum der WEG-Gruppe verletzen. Ebenso ist der Zugang zu oder die Verbreitung von illegalen, pornografischen Inhalten jeglicher Art oder von Inhalten, die gegen das Kinder- und Jugendstatut verstoßen, nicht gestattet;

- Die dem Partner zur Verfügung gestellten Zugangsdaten sind ausschließlich zur Nutzung bestimmt und dürfen nicht weitergegeben oder mit anderen geteilt werden;
- Der Partner ist verpflichtet, seine Zugangsdaten sicher aufzubewahren, und er trägt die alleinige und ausschließliche Verantwortung für jede Nutzung seiner Zugangsdaten, einschließlich eines etwaigen Missbrauchs;
- Es liegt in der Verantwortung des Partners, jede Entlassung von Mitarbeitern, Lieferanten oder Dienstleistern mitzuteilen.

6.1.2. Benachrichtigung über Vorfälle der Informationssicherheit

Wenn der Partner einen Vorfall entdeckt oder den begründeten Verdacht hat, dass ein Vorfall stattfindet oder stattgefunden hat, muss er:

- Unverzügliche Einleitung der Vorfallsbehandlung, um gefährdete IT-Systeme und Unternehmensdaten zu untersuchen, umgehend einzudämmen und zu schützen sowie die Auswirkungen des Vorfalls auf die IT-Systeme zu minimieren und abzuschwächen;
- Unverzügliche Benachrichtigung der WEG-Gruppe per E-Mail an soc@weg.net.

Der Partner muss den Vorfall unter Angabe der folgenden Informationen melden:

- Art und vermuteter Umfang des Vorfalls;
- Das verdächtige Datum, an dem der Vorfall begann;
- Datum und Uhrzeit der Entdeckung des Vorfalls;
- Maßnahmen, die der Partner ergriffen hat, um die weitere Bereitstellung des Umfangs zu gewährleisten und gegebenenfalls die Unternehmensdaten zu schützen und wiederherzustellen; und
- Kontaktdaten eines Vertreters des Partners, der auf Anfragen der WEG-Gruppe zu diesen Informationen antwortet.

Der Partner muss der WEG-Gruppe so schnell wie möglich die folgenden Informationen zur Verfügung stellen:

- die vermutete(n) Ursache(n) des Vorfalls und den/die beteiligten Akteur(en);
- die geschätzten Auswirkungen des Vorfalls;
- Vorgeschlagene Abhilfemaßnahmen und geschätzte Zeit bis zur vollständigen Erholung von den Auswirkungen des Vorfalls; und
- Vorgeschlagene Abhilfemaßnahmen, einschließlich der Sicherstellung der weiteren Bereitstellung des Umfangs und des Schutzes und der Wiederherstellung von Unternehmensdaten, sofern relevant.

Der Partner stellt der WEG-Gruppe regelmäßig aktualisierte Informationen gemäß den vorstehenden Absätzen sowie alle anderen Informationen zur Verfügung, die die WEG-Gruppe im Zusammenhang mit dem Vorfall vernünftigerweise anfordert (einschließlich Aufzeichnungen über alle Zugriffe auf die betreffenden IT-Systeme im Zusammenhang mit dem Vorfall und Nachweise für den wirksamen Schutz und die Wiederherstellung der Daten des Unternehmens).

Der Partner stellt der WEG-Gruppe unverzüglich jede Unterstützung zur Verfügung, die die WEG-Gruppe benötigt, um Vorfälle zu untersuchen, auf sie zu reagieren, ihre Auswirkungen zu mindern und sie zu beheben (einschließlich des Schutzes und der Wiederherstellung von Unternehmensdaten) und um mit Einzelpersonen oder Behörden, einschließlich der zuständigen Regulierungsbehörden, zu kommunizieren und ihnen zu antworten.

Der Partner stellt der WEG-Gruppe einen Abschlussbericht über den Vorfall, einschließlich einer Ursachenanalyse, zur Verfügung, sobald dieser verfügbar ist.
Ungeachtet anderslautender Bestimmungen im Vertrag gilt ein Zwischenfall nicht als Ereignis höherer Gewalt, wenn er auf einen Verstoß gegen diesen Anhang oder auf Fahrlässigkeit eines Mitglieds des Partners zurückzuführen ist.

6.1.3. Sicherheit der Ausrüstung

- Jeder Partner ist für den Schutz der physischen Geräte verantwortlich, die Informationen der WEG-Gruppe enthalten und sich in seinem Gewahrsam befinden; und
- Die Partner sind sich darüber im Klaren, dass der Zugang zu einer Umgebung der WEG-Gruppe oder die Nutzung einer IT-Ressource in der Umgebung der WEG-Gruppe, selbst wenn der Partner persönliche Geräte verwendet, der Überwachung und Inspektion unterliegt, es sei denn, das geltende lokale Recht verbietet ein solches Verhalten ausdrücklich.

6.1.4. Verstoß gegen die Verhaltensregeln

Die folgenden Situationen werden als Verstöße gegen diese Informationssicherheitsrichtlinie für Partner angesehen, ohne darauf beschränkt zu sein:

- Jegliche Handlungen, Unterlassungen oder andere Situationen, die die WEG-Gruppe direkt oder indirekt, potenziell oder tatsächlich, einem finanziellen oder Imageverlust aussetzen können, der ihre Informationswerte gefährdet;
- Missbrauch oder Offenlegung von Informationen ohne die ausdrückliche Genehmigung der WEG-Gruppe, wie z. B. Unternehmensdaten, Geschäftsgeheimnisse oder andere Informationen;
- Die begangene oder unterlassene Nichteinhaltung von Richtlinien, Regeln, Parametern oder Verpflichtungen, die in dieser Informationssicherheitspolitik für Partner festgelegt sind;
- Nutzung von Daten, Informationen, Geräten, Software, Systemen oder anderen technologischen Ressourcen für unerlaubte Zwecke, wozu auch die Verletzung von Gesetzen, internen und externen Vorschriften, ethischen Grundsätzen oder Anforderungen von Aufsichtsbehörden im Tätigkeitsbereich der WEG-Gruppe gehören kann; und
- Das Versäumnis, der WEG-Gruppe alle Vorfälle im Bereich der Informationssicherheit oder die Nichteinhaltung dieser Informationssicherheitspolitik für Partner unverzüglich mitzuteilen.

6.2. SICHERHEITS- UND DATENSCHUTZKONTROLLEN IN DER PARTNERUMGEBUNG

Auf Anfrage des Geschäftsbereichs der WEG-Gruppe wird der betreffende Partner vom Information Security Governance-Team in einem Tool registriert, um seine Cyber-Gesundheit zu überprüfen. Auf dieser Plattform werden Punkte vergeben.
Die Gesamtpunktzahl des Partners muss mindestens 80 % oder die vom Tool selbst angegebene Durchschnittspunktzahl seines Marktsegments erreichen, je nachdem, welcher Wert höher ist.
Partner, die die angestrebte Punktzahl nicht erreichen, erhalten von der WEG-Gruppe einen Bericht über die Angemessenheit und Einhaltung der Vorschriften, so dass der Partner Maßnahmen ergreifen kann, um die angestrebte Punktzahl innerhalb von 180 Tagen zu erreichen.

Zusätzlich zu dem oben beschriebenen Registrierungsverfahren muss der Partner die folgenden Richtlinien zur Informationssicherheit befolgen, die auch in dem vom Bereich Informationssicherheit übermittelten und verwalteten Dokument zur Selbsteinschätzung vorgesehen sind.

6.2.1. Datenschutz

- Dokumentieren Sie den Fluss der WEG-Daten in der Umgebung des Partners, einschließlich des gesamten Lebenszyklus (Erhebung, Verarbeitung, Speicherung, Weitergabe und Löschung).
- die WEG-Gruppe darüber informieren, welche Daten zu welchem Zweck erhoben werden, auf welcher Rechtsgrundlage die Daten verarbeitet werden, wo und wie lange sie gespeichert werden, wobei stets versucht wird, die Speicherdauer und die Menge der erhobenen Daten zu minimieren.
- Eine Folgenabschätzung in Bezug auf die personenbezogenen Daten des Inhabers (DPIA) sowie ein Verfahren, das der WEG-Gruppe uneingeschränkten Zugang zu den verarbeiteten und gespeicherten Daten gewährt, sind im Rahmen des Vertrags vorgesehen.
- Über ein Opt-in und Opt-out-Verfahren für die vorherige und freie Äußerung der WEG-Gruppe und der Inhaber personenbezogener Daten über die gemeinsame Nutzung im Rahmen einer Partnerschaft verfügen. Es ist auch zu beachten, dass die Standardeinstellung die Nichtweitergabe sein sollte. Erst nach dem Opt-in der betroffenen Partei kann der Partner Daten mit Partnern teilen.

6.2.2. Zugangskontrolle

- Über ein ordnungsgemäß dokumentiertes Zugangsmanagementverfahren verfügen;
- Der WEG-Gruppe einen uneingeschränkten Zugang zu den gespeicherten oder zu verarbeitenden Daten und Informationen zu gewähren, entsprechend den definierten spezifischen Dienstleistungen, unter Berücksichtigung der Vertraulichkeit, Integrität, Verfügbarkeit und Wiederherstellbarkeit dieser Daten und Informationen;
- Transparenz für die WEG-Gruppe in Bezug auf die Verfahren und Kontrollen, die zur Einhaltung des Vertrags eingesetzt werden, wie im obigen Punkt beschrieben, insbesondere für die Identifizierung und Trennung der Kundendaten der WEG-Gruppe durch physische oder logische Kontrollen;
- Keine Verwendung von gemeinsamen Konten oder allgemeinen Benutzern für kritische Systeme zulassen und Kontrollen in Bezug auf die Anmeldung beibehalten, wie z. B. (aber nicht beschränkt auf): Änderungen beim ersten Zugriff erzwingen, den Benutzer nach einer bestimmten Anzahl von ungültigen Versuchen sperren, komplexe Passwortmuster und andere Informationssicherheitspraktiken in Übereinstimmung mit den besten Marktstandards verlangen;
- über ein formalisiertes und dokumentiertes Verfahren für die Gewährung, Änderung und den Entzug von Zugriffsrechten verfügen, insbesondere von solchen mit privilegierten Anteilen;
- über ein Verfahren zur Kontrolle der fehlenden Funktionstrennung (SOD) verfügen;
- Einführung einer Politik der geringsten Privilegien;
- über Methoden für die physische und logische Zugangskontrolle von Besuchern verfügen; und
- Fernzugriffskontrollen für Mitarbeiter/Dienstleister während Telearbeitsphasen.

6.2.3. Überwachung der Dienste und Verwaltung der Informationssicherheitsmaßnahmen

- Sicherstellen, dass er über ein Höchstmaß an Kapazitäten für die Bereitstellung von Informationen und angemessenen Managementressourcen zur Überwachung der zu erbringenden Dienstleistungen verfügt und die Einhaltung der geltenden Gesetze und Vorschriften gewährleistet;
- I die WEG-Gruppe auf Anfrage über die geeigneten Managementressourcen für die Überwachung der beauftragten Dienstleistungen zu informieren und ihr Zugang dazu zu gewähren;
- Sie verfügen über Ressourcen und Tools zur Überwachung der Kapazität und Verfügbarkeit Ihrer Anlagen, zur Korrelation von Warnungen und zur automatischen Erstellung von Tickets für Vorfälle;
- über einen strukturierten Incident-Response-Prozess verfügen, einschließlich der Kategorisierung von Vorfällen und Runbooks für den Umgang mit bekannten Vorfällen und deren Behebung.
- Vorfälle im Zusammenhang mit der Cyber-Umgebung zu verhindern, zu erkennen und zu reduzieren, wobei Verfahren und Kontrollen nachzuweisen sind, die zumindest Authentifizierung, Verschlüsselung, Verhinderung und Erkennung von Eindringlingen, Verhinderung von Datenlecks, regelmäßige Tests und Scans zur Erkennung von Schwachstellen, Anwendung von Sicherheits-Patches, Anwendung von Härtungsmaßnahmen auf seinen Servern und Workstations, Schutz vor bösartiger Software und Blockierung nicht zugelassener Software, Einrichtung von Rückverfolgbarkeits- und Segmentierungsmechanismen für das Computernetzwerk, Pflege von Daten- und Informationssicherheitskopien umfassen;
- WEG behält sich das Recht vor, im Falle eines Sicherheitsvorfalls oder eines anormalen/unangemessenen Verhaltens in der WEG-Umgebung, in das der Partner verwickelt ist, unverzüglich und einseitig den Zugang zu sperren, unabhängig davon, ob dieser Vorfall bestätigt wurde, ein Verdacht besteht oder eine Untersuchung läuft;
- auf Anfrage Informationen über die Anzahl der in den letzten 24 Monaten aufgetretenen Vorfälle vorzulegen und diese nach ihrer Relevanz zu klassifizieren. Alle Daten über Vorfälle von „mittlerem“, „hohem“ oder „sehr hohem“ Schweregrad müssen vom Partner mindestens 5 Jahre lang aufbewahrt werden; und
- die WEG-Gruppe ständig über alle Einschränkungen zu informieren, die sich auf die Erbringung von Dienstleistungen oder die Einhaltung der geltenden Gesetze und Vorschriften auswirken können.

6.2.4. Management von Bedrohungen

Der Partner stellt sicher, dass Schwachstellen in IT-Systemen rechtzeitig gepatcht oder aktualisiert werden. In jedem Fall muss der Partner:

a) Innerhalb von 24 Stunden nach der Entdeckung einer kritischen Schwachstelle (CVSS oder CVE 9.0 oder höher) in den betreffenden IT-Systemen der vertragschließenden Gruppe, die nicht von einem Dritten bereitgestellt wird:

- Beginnen Sie mit der Entwicklung und Bereitstellung eines Updates oder Patches zur Behebung der Sicherheitslücke;
- Benachrichtigung der WEG-Gruppe unter soc@weg.net und Angabe von Einzelheiten über die Sicherheitslücke und die damit verbundene Bedrohung sowie der Maßnahmen, die der Partner zur Behebung der Bedrohung oder der Sicherheitslücke ergriffen hat.

- Sicherstellen, dass auf allen relevanten IT-Systemen des Partners die neuesten von Dritten zur Verfügung gestellten Patches installiert und eingesetzt werden; und
- Installation und Bereitstellung von Updates oder Patches für Schwachstellen, die im Katalog der U.S. Cyber & Infrastructure Security Agency für bekannte ausgenutzte Schwachstellen enthalten sind, innerhalb von 24 Stunden nach Veröffentlichung des Updates oder Patches. Wenn ein Update oder Patch aus irgendeinem Grund nicht innerhalb von 24 Stunden eingespielt werden kann, muss der Partner die WEG-Gruppe unverzüglich unter soc@weg.net informieren.

b) Der Partner muss:

- sicherstellen, dass die relevanten IT-Systeme kontinuierlich überwacht werden, um ihre Sicherheit, Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten; und
- Kontinuierlich die relevanten IT-Systemprotokolle erstellen, die erforderlich sind, um: (A) die Reaktion auf Vorfälle zu ermöglichen; (B) die Quelle eines Vorfalls zu identifizieren; und (C) die Abfolge der Ereignisse, die zu einem Vorfall geführt haben, zu rekonstruieren. Der Partner muss diese Aufzeichnungen mindestens 180 Tage lang ab dem Datum der Erstellung sicher aufbewahren, so dass nur autorisierte Benutzer auf diese Aufzeichnungen zugreifen können.

6.2.5. Sicherheit in der Systementwicklung

- Führen Sie in Ihren Softwareentwicklungsprozessen Verfahren zum Schutz der Privatsphäre und zum „Security by Design“ ein;
- Beschreiben Sie die Sicherheitsmerkmale und Daten, auf die die Anwendungen zugreifen, die vom Bereich Informationssicherheit während der Genehmigungsphase bewertet werden müssen (Beispiel: Technische Spezifikation und/oder Funktionsdiagramm);
- Einsatz von Integritätsprüfungsroutinen zur Vermeidung von Fehlern, ob unfreiwillig oder absichtlich, unter Verwendung fiktiver Daten oder Anonymisierungen in einer nicht produktiven Umgebung;
- Übernahme von Sicherheitsanalyseverfahren in den Quellcode;
- Anwendung von Praktiken zur Sicherheitsanalyse in ihren Anwendungen (Ethical Hacking Tests und Penetrationstests);
- Sicherheitsvalidierungen im Rahmen der Codequalität und des Verifikationsprozesses vorsehen. Zumindest sollten diejenigen berücksichtigt werden, die in den OWASP TOP 10 aufgeführt sind.

6.2.6. Geschäftskontinuität, Datenmanagement, Aufbewahrung und Speicherung

- Definition eines Business-Continuity-Programms, um sicherzustellen, dass mögliche Vorfälle die für die WEG-Gruppe erbrachten Dienstleistungen nicht beeinträchtigen, insbesondere unter Berücksichtigung des Disaster-Recovery-Plans, und regelmäßige Tests der Sicherheitskontrollen, um zu überprüfen, wie gut das Unternehmen auf reale Fälle vorbereitet ist;
- die WEG-Gruppe auf Anfrage über die Sicherheitsmaßnahmen für die Übermittlung und Speicherung von Daten und Informationen sowie deren Entsorgung zu informieren und ihr Zugang dazu zu gewähren, wobei sichere Ausschlussverfahren (digital und/oder physisch) anzuwenden sind;

- über ein Backup-Verfahren zu verfügen, das in regelmäßigen Abständen für die Anlagen, auf denen Informationen der WEG-Gruppe gespeichert sind, durchgeführt wird, um Datenverluste bei Zwischenfällen zu vermeiden oder zu minimieren.

6.2.7. Schulung und Sensibilisierung

- Gewährleistung eines Schulungs- und Sensibilisierungsprogramms in den Bereichen Informationssicherheit und Datenschutz, das mindestens einmal jährlich für alle Mitarbeiter, Lieferanten und Dienstleister durchgeführt wird, wobei die Schulung mit der obligatorischen Anwendung des Partner-Verhaltenskodex für neu eingestellte Mitarbeiter, Lieferanten und Dienstleister einhergehen muss.
- In sein Schulungs- und Sensibilisierungsprogramm für Informationssicherheit und Datenschutz sind Kampagnen zur Verhinderung von Phishing und Anleitungen zum Social Engineering sowie Vorträge, die Herausgabe von Newslettern zu Informationssicherheit und Datenschutz usw. aufzunehmen.
- Die Mitarbeiter, Lieferanten und Dienstleister der Partner, die Zugang zu personenbezogenen Daten und/oder sensiblen Informationen haben oder diese verarbeiten, müssen sich dieser Richtlinie bewusst sein und wissen, wovon die Informationssicherheitsschulung handelt.

6.2.8. Dienstleistungen und Zertifizierungen

Der Partner muss:

- die Vergabe von Unteraufträgen für Dienstleistungen, die für den Gegenstand des Vertrags mit der WEG-Gruppe relevant sind, im Voraus und formell melden;
- über Anerkennungen im Bereich der Informationssicherheit oder der Geschäftskontinuität verfügen, die durch unabhängige externe Prüfberichte nachgewiesen werden;
- die WEG-Gruppe auf Anfrage über die für die Erbringung der Dienstleistungen erforderlichen Zertifizierungen sowie über die von einer spezialisierten unabhängigen Wirtschaftsprüfungsgesellschaft erstellten Berichte über die bei der Erbringung der vertraglich vereinbarten Dienstleistungen eingesetzten Kontrollen informieren und ihr Zugang dazu gewähren; und
- über Mechanismen zur Meldung von Anomalien oder Sicherheitsvorfällen an die WEG-Gruppe, die betroffenen Personen und die nationale Datenschutzbehörde verfügen.

7. PERIODISCHE EVALUIERUNGEN

Die WEG-Gruppe kann, wann immer sie es für notwendig erachtet, Bewertungen durchführen, um die Wirksamkeit der Umsetzung der in diesem Dokument dargelegten Kontrollen zu bescheinigen, und muss den Partner zu diesem Zweck 30 Tage im Voraus informieren. Evaluierungen können auch im Falle eines Sicherheitsvorfalls oder einer Änderung der für das Segment des Partners oder der WEG-Gruppe geltenden Marktbedingungen erfolgen.

8. SANKTIONEN

Die Verletzung einer Kontrolle oder die Nichteinhaltung der Informationssicherheitsrichtlinie für Partner und ihrer Definitionen werden als schwerwiegende Fehler oder Verstöße betrachtet, und es können gemäß den internen Richtlinien der WEG-Gruppe und/oder gemäß den vertraglichen Bestimmungen entsprechende Strafen oder Sanktionen verhängt werden.

Im Falle eines Verstoßes gegen eine Verpflichtung oder Bestimmung dieser Richtlinie durch den Partner, seine Mitarbeiter, Lieferanten, Dienstleister und/oder mit dem Partner verbundene Personen verpflichtet sich der Partner, die WEG-Gruppe unbeschadet anderer vertraglich oder gesetzlich vorgesehener Strafen, Sanktionen und/oder Bußgelder für alle Verluste oder Schäden zu entschädigen, schadlos zu halten, zu verteidigen und schadlos zu halten.

Der Partner erkennt an und erklärt sich damit einverstanden, dass eine bloße Entschädigung möglicherweise nicht das geeignete Mittel ist, um Verstöße gegen diese Richtlinie zu beheben, und dass die WEG-Gruppe jede Form und/oder jedes Mittel zur spezifischen Erfüllung von Verpflichtungen anwenden kann, die im Falle eines drohenden oder tatsächlichen Verstoßes gegen diese Partnerschaft anwendbar sein können.