قرارداد خدمات ارزیابی جامع امنیت شبکه

این قرارداد، مابین شرکت [نام کامل کارفرما]، ثبت شده به شماره ثبت [شماره ثبت کارفرما] در اداره ثبت شرکت‌ها با شناسه ملی [شناسه ملی کارفرما]، به نشانی [آدرس دقیق و کامل پستی کارفرما]، کد پستی [کد پستی کارفرما]، که در این قرارداد «کارفرما» نامیده می‌شود، از یک طرف، و شرکت [نام کامل مجری ارزیابی]، ثبت شده به شماره ثبت [شماره ثبت مجری] در اداره ثبت شرکت‌ها با شناسه ملی [شناسه ملی مجری]، دارای پروانه فعالیت از [نام مرجع صدور پروانه، مثلاً سازمان نظام صنفی رایانه‌ای/وزارت ارتباطات و فناوری اطلاعات]، به نشانی [آدرس دقیق و کامل پستی مجری]، کد پستی [کد پستی مجری]، با شماره تماس [شماره تماس مجری] و پست الکترونیک [پست الکترونیک مجری]، که در این قرارداد «مجری» نامیده می‌شود، از طرف دیگر، در تاریخ [روز] / [ماه] / [سال] شمسی، مطابق با [تاریخ میلادی معادل]، منعقد و لازم‌الاجرا می‌گردد.

پیش‌گفتار (بند مقدمه):

نظر به اهمیت روزافزون امنیت اطلاعات و شبکه‌های کامپیوتری در حفظ دارایی‌های فکری، اطلاعات حساس تجاری، و تداوم کسب‌وکار، و با عنایت به ضرورت شناسایی و رفع مؤثر آسیب‌پذیری‌های احتمالی در زیرساخت‌های شبکه کارفرما، طرفین با اراده کامل و اختیار تام، این قرارداد را جهت بهره‌مندی از خدمات تخصصی ارزیابی امنیت شبکه که توسط مجری ارائه می‌گردد، منعقد می‌نمایند. مفاد این قرارداد، چارچوب قانونی و فنی روابط طرفین را در خصوص موضوع قرارداد تعیین می‌نماید.

ماده ۱: تعاریف

در این قرارداد، واژگان و اصطلاحات زیر، مفاهیم مشروحه ذیل را خواهند داشت، مگر آنکه در متن صراحتاً خلاف آن ذکر شده باشد:

۱٫۱. **شبکه:** کلیه تجهیزات سخت‌افزاری (سرورها، روترها، سوئیچ‌ها، فایروال‌ها، دستگاه‌های ذخیره‌سازی، ایستگاه‌های کاری، دستگاه‌های سیار، تجهیزات IoT و غیره)، نرم‌افزاری (سیستم‌عامل‌ها، سرویس‌ها، برنامه‌های کاربردی، پایگاه‌های داده) و ارتباطات (سیمی، بی‌سیم، VPN) که به هم متصل بوده و امکان تبادل اطلاعات را دارند و متعلق به کارفرما می‌باشند.

۱٫۲. **آسیب‌پذیری (Vulnerability):** ضعفی در طراحی، پیاده‌سازی، عملیات یا مدیریت یک سیستم که می‌تواند توسط یک تهدید مورد سوءاستفاده قرار گیرد و منجر به نقض سیاست‌های امنیتی شود.

۱٫۳. **تهدید (Threat):** عاملی بالقوه که می‌تواند به یک سیستم یا سازمان آسیب برساند، مانند بدافزار، دسترسی غیرمجاز، یا حملات انکار سرویس.

۱,۴. **ریسک (Risk)**: احتمال وقوع یک رویداد تهدیدآمیز و پیامدهای ناشی از آن بر روی دارایی‌های سازمان. ریسک معمولاً به صورت حاصل‌ضرب احتمال وقوع (Likelihood) در شدت تأثیر (Impact) محاسبه می‌شود.

۱,۵. **تست نفوذ (Penetration Testing)**: فرآیندی شبیه‌سازی شده و مجاز برای ارزیابی امنیت یک سیستم یا شبکه با تلاش فعالانه برای یافتن و سوءاستفاده از آسیب‌پذیری‌ها.

۱,۶. **ارزیابی امنیتی (Security Assessment)**: فرآیندی جامع‌تر که ممکن است شامل تست نفوذ، اسکن آسیب‌پذیری، بررسی پیکربندی، و بازبینی مستندات و سیاست‌ها باشد.

۱,۷. **گزارش جامع**: مستند نهایی که توسط مجری تهیه و حاوی یافته‌ها، تحلیل ریسک‌ها، و پیشنهادات عملیاتی است.

۱,۸. **دامنه ارزیابی (Scope of Assessment)**: مجموعه‌ای از دارایی‌ها، سیستم‌ها، شبکه‌ها، و برنامه‌های کاربردی که صراحتاً در این قرارداد برای ارزیابی مشخص شده‌اند.

۱,۹. **تیم ارزیابی**: افراد متخصص و آموزش‌دیده از جانب مجری که مسئولیت اجرای فنی ارزیابی را بر عهده دارند.

۱,۱۰. **دوره تضمین**: دوره‌ای مشخص پس از تحویل گزارش نهایی که طی آن مجری مسئول بررسی مجدد و رفع اشکال در یافته‌های گزارش شده است.

ماده ۲: موضوع قرارداد

۲,۱. موضوع اصلی این قرارداد، انجام خدمات جامع ارزیابی امنیت شبکه اطلاعاتی کارفرما، شامل شناسایی کلیه دارایی‌های تحت پوشش، کشف و تحلیل آسیب‌پذیری‌ها، ارزیابی ریسک‌های مرتبط، شبیه‌سازی حملات سایبری مجاز (تست نفوذ)، و ارائه یک گزارش جامع فنی و مدیریتی به همراه پیشنهادات عملیاتی و اولویت‌بندی شده جهت ارتقاء سطح امنیت، کاهش ریسک‌ها و حفاظت از دارایی‌های اطلاعاتی کارفرما می‌باشد.

۲,۲. دامنه دقیق خدمات و دارایی‌های مشمول ارزیابی، در **پیوست الف** (Scope of Work) این قرارداد که جزئی جدایی‌ناپذیر از آن است، به تفصیل مشخص و تعیین خواهد گردید. این پیوست شامل لیست IP Address ها، نام دامنه‌ها، سرویس‌های خاص، برنامه‌های کاربردی، و سطوح دسترسی مورد نظر برای ارزیابی خواهد بود.

ماده ۳: دامنه دقیق خدمات و تعهدات تفصیلی مجری

مجری متعهد می‌گردد خدمات ارزیابی امنیت شبکه را با بالاترین استانداردهای فنی و حرفه‌ای، مطابق با چارچوب‌های معتبر بین‌المللی (مانند NIST SP 800-115, OWASP Testing Guide, PTES - Penetration Testing Execution Standard, ISO/IEC 27001/27002) و با رعایت اصول اخلاقی حرفه‌ای، به شرح ذیل و مطابق با پیوست الف انجام دهد:

۳,۱. **مرحله آماده‌سازی و شناسایی (Preparation & Reconnaissance):**

۳,۱,۱. **برنامه‌ریزی و هماهنگی:** تشکیل جلسات توجیهی با کارفرما، تعریف دقیق دامنه، اهداف، محدودیت‌ها، زمان‌بندی، و قوانین درگیری (Rules of Engagement - RoE) تست.

۳,۱,۲. **شناسایی غیرفعال (Passive Reconnaissance):** جمع‌آوری اطلاعات در مورد کارفرما و زیرساخت‌های آن از منابع عمومی (مانند WHOIS, DNS records, Public databases) بدون تعامل مستقیم با شبکه هدف.

۳,۱,۳. **شناسایی فعال (Active Reconnaissance):** تعامل مستقیم با شبکه هدف جهت شناسایی دقیق دارایی‌ها، پورت‌های باز، سرویس‌های فعال، و سیستم‌عامل‌ها. این شامل تکنیک‌هایی مانند Port Scanning (TCP/UDP), Banner Grabbing, OS Fingerprinting, Network Mapping, و Service Enumeration می‌باشد.

۳,۱,۴. **شناسایی دارایی‌های شبکه (Inventory & Asset Discovery):** تهیه یک لیست جامع و دقیق از کلیه تجهیزات سخت‌افزاری، نرم‌افزاری، و سرویس‌های فعال شناسایی شده در دامنه ارزیابی.

۳,۲. **مرحله تحلیل و ارزیابی آسیب‌پذیری (Assessment & Vulnerability Analysis):**

۳,۲,۱. **اسکن خودکار آسیب‌پذیری (Automated Vulnerability Scanning):** استفاده از ابزارهای استاندارد و به‌روز (مانند Nessus, Qualys, OpenVAS) جهت شناسایی خودکار آسیب‌پذیری‌های شناخته شده در سیستم‌عامل‌ها، برنامه‌های کاربردی، و سرویس‌های شبکه.

۳,۲,۲. **تحلیل نتایج اسکن:** بررسی و اعتبارسنجی نتایج حاصل از اسکن‌های خودکار، حذف هشدارهای کاذب (False Positives)، و اولویت‌بندی آسیب‌پذیری‌ها بر اساس شدت و سطح ریسک.

۳,۲,۳. **تحلیل دستی آسیب‌پذیری (Manual Vulnerability Analysis):** بررسی عمیق‌تر آسیب‌پذیری‌هایی که نیاز به تحلیل تخصصی دارند و اسکنرهای خودکار قادر به کشف کامل آن‌ها نیستند.

۳,۲,۴. **تحلیل پیکربندی امنیتی (Security Configuration Review):** بررسی تنظیمات امنیتی کلیدی تجهیزات شبکه (مانند فایروال‌ها، روترها، سوئیچ‌ها)، سرورها (ویندوز، لینوکس)، و سرویس‌های مهم (مانند Active Directory, Web Servers, Database Servers) بر اساس بهترین شیوه‌ها (Best Practices) و استانداردهای امنیتی. این شامل بررسی سیاست‌های رمز عبور، دسترسی‌ها، لاگ‌برداری، به‌روزرسانی‌ها، و بستن سرویس‌های غیرضروری است.

۳,۲,۵. **ارزیابی امنیت پروتکل‌ها و سرویس‌ها:** شناسایی و ارزیابی امنیتی سرویس‌های پروتکل‌های ارتباطی رایج (مانند HTTP/S, FTP, SSH, Telnet, RDP, SMB, DNS, SMTP, SNMP) و پروتکل‌های احراز هویت.

۳,۲,۶. **ارزیابی امنیت شبکه بی‌سیم (Wi-Fi Security Assessment)**: در صورت وجود در دامنه، شناسایی نقاط دسترسی بی‌سیم، تحلیل پروتکل‌های رمزنگاری (WEP, WPA/WPA2/WPA3)، و تلاش برای دسترسی غیرمجاز.

۳,۳. **مرحله بهره‌برداری و تست نفوذ (Penetration Testing & Exploitation)**:

۳,۳,۱. **تست نفوذ خارجی (External Penetration Testing)**: تلاش برای نفوذ به شبکه از دید یک مهاجم خارجی که هیچ دسترسی داخلی ندارد. این شامل کشف و بهره‌برداری از آسیب‌پذیری‌های قابل دسترس از اینترنت (مانند آسیب‌پذیری‌های وب سرورها، سرویس‌های VPN، تجهیزات لبه شبکه) است.

۳,۳,۲. **تست نفوذ داخلی (Internal Penetration Testing)**: شبیه‌سازی سناریوهای حمله از دید یک مهاجم که به طور اولیه به شبکه داخلی دسترسی یافته است (مانند یک ایستگاه کاری آلوده، یک حساب کاربری داخلی به خطر افتاده). این مرحله بر کشف آسیب‌پذیری‌های داخلی، افزایش سطح دسترسی (Privilege Escalation)، حرکت جانبی (Lateral Movement)، و دسترسی به داده‌های حساس تمرکز دارد.

۳,۳,۳. **تست نفوذ وب اپلیکیشن (Web Application Penetration Testing)**: تمرکز بر ارزیابی امنیت برنامه‌های کاربردی تحت وب (مانند پورتال‌ها، پنل‌های مدیریت، API ها) با استفاده از تکنیک‌های استاندارد (مانند OWASP Top 10) جهت کشف آسیب‌پذیری‌هایی چون SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Insecure Direct Object References, Security Misconfiguration و غیره.

۳,۳,۴. **تست نفوذ API**: ارزیابی امنیت رابط‌های برنامه‌نویسی کاربردی (API) که توسط برنامه‌های کاربردی یا سرویس‌های دیگر استفاده می‌شوند.

۳,۳,۵. **تست مهندسی اجتماعی (Social Engineering Testing – در صورت توافق و با رعایت محدودیت‌ها)**: شبیه‌سازی حملات مهندسی اجتماعی (مانند فیشینگ هدفمند) بر روی تعداد محدودی از کاربران، به منظور ارزیابی سطح آگاهی امنیتی و مقاومت در برابر این نوع حملات. این بخش نیازمند رضایت کتبی صریح و دقیق کارفرما و تعریف شفاف سناریوها و محدودیت‌ها است.

۳,۳,۶. **سایر تست‌های تخصصی (بسته به دامنه)**: بسته به نیاز، ممکن است تست‌هایی چون ارزیابی امنیت پایگاه داده، تست نفوذ اپلیکیشن‌های موبایل، یا تست امنیت سیستم‌های SCADA/ICS نیز در دامنه قرار گیرند.

۳,۴. **مرحله تحلیل ریسک و اولویت‌بندی**:

۳,۴,۱. **تحلیل سطح ریسک**: ارزیابی پیامدهای احتمالی هر آسیب‌پذیری کشف شده بر اساس معیارهای کسب‌وکار کارفرما (مانند خسارت مالی، نقض قوانین، خدشه‌دار شدن اعتبار، اختلال در عملیات) و احتمال وقوع سوءاستفاده از آن.

۳,۴,۲. **طبقه‌بندی ریسک**: دسته‌بندی ریسک‌ها به سطوح مختلف (مانند بحرانی، بالا، متوسط، پایین، اطلاعاتی) بر اساس متدولوژی‌های استاندارد (مانند CVSS - Common Vulnerability Scoring System).

۳,۴,۳. **اولویت‌بندی پیشنهادات:** ارائه لیستی از پیشنهادات اصلاحی بر اساس اولویت رفع ریسک‌های بحرانی و بالا، و همچنین در نظر گرفتن سهولت پیاده‌سازی و هزینه.

۳,۵. **مرحله گزارش‌دهی و ارائه نتایج:**

۳,۵,۱. **تدوین گزارش جامع:** تهیه دو بخش اصلی گزارش:

الف) **خلاصه مدیریتی (Executive Summary):** متنی مختصر و سطح بالا که برای مدیران ارشد و تصمیم‌گیرندگان غیرفنی طراحی شده است. شامل تشریح کلی وضعیت امنیت، مهم‌ترین ریسک‌ها، و توجیه کلی سرمایه‌گذاری لازم برای بهبود امنیت.

ب) **گزارش فنی (Technical Report):** متنی جامع و دقیق که برای تیم فنی و امنیتی کارفرما تهیه شده است. شامل جزئیات کامل دامنه ارزیابی، متدولوژی مورد استفاده، تشریح فنی کلیه آسیب‌پذیری‌های کشف شده، مستندات اثبات (Proof of Concept)، نتایج تحلیل ریسک، و پیشنهادات اصلاحی عملیاتی و گام به گام.

۳,۵,۲. **مستندات اثبات (Evidence):** ارائه شواهد کافی و قابل قبول برای هر یافته امنیتی، مانند اسکرین‌شات‌ها، لاگ‌ها، درخواست‌ها و پاسخ‌های شبکه، و مثال‌های کد (در صورت لزوم).

۳,۵,۳. **ارائه حضوری گزارش:** برگزاری جلسه ارائه نتایج با حضور نمایندگان فنی و مدیریتی کارفرما، تشریح گزارش، پاسخ به سوالات، و بحث پیرامون اولویت‌بندی اقدامات اصلاحی.

ماده ۴: تعهدات تفصیلی کارفرما

کارفرما متعهد می‌گردد حداکثر همکاری لازم را با مجری در طول اجرای پروژه به عمل آورد:

۴,۱. **تعیین نماینده و تیم پشتیبان:** معرفی یک یا چند نماینده تام‌الاختیار (Technical Point of Contact - POC) که مسئولیت هماهنگی‌های فنی، پاسخگویی به استعلامات، و تصمیم‌گیری‌های مرتبط با دامنه و زمان‌بندی را بر عهده خواهند داشت. همچنین، فراهم آوردن دسترسی لازم به اعضای تیم فنی و امنیتی کارفرما جهت تسهیل فرآیند ارزیابی.

۴,۲. **فراهم آوردن دسترسی‌های لازم:**

الف) **دسترسی‌های Read-Only:** در صورت امکان و توافق، فراهم آوردن دسترسی‌های فقط خواندنی (Read-Only) به سیستم‌ها و ابزارهای مدیریتی شبکه جهت تسریع فرآیند شناسایی و تحلیل.

ب) **دسترسی به مستندات:** در اختیار قرار دادن مستندات مرتبط با معماری شبکه، لیست تجهیزات، نقشه‌ها، و سیاست‌های امنیتی موجود (در صورت وجود و تمایل).

ج) **دسترسی مدیریتی (در صورت نیاز):** در برخی مراحل تست نفوذ (مانند افزایش سطح دسترسی)، ممکن است نیاز به دسترسی‌های مدیریتی موقت و کنترل شده باشد که این موضوع باید به صورت صریح در دامنه توافق شود.

۴,۳. **تعریف دقیق دامنه و محدودیت‌ها:** ارائه مشخصات دقیق دارایی‌های مشمول ارزیابی (IP ها، دامنه‌ها، اپلیکیشن‌ها) و تعیین دقیق هرگونه محدودیت زمانی، جغرافیایی، یا فنی در انجام تست‌ها (مثلاً عدم تست در ساعات اوج کاری، عدم انجام حملات DoS/DDoS، عدم تست بر روی سیستم‌های حساس تولیدی). این موارد باید در پیوست الف به طور شفاف ذکر شوند.

۴,۴. **تأمین زیرساخت تست (در صورت نیاز):** در برخی سناریوها، ممکن است نیاز به ایجاد یک محیط تست مجزا یا فراهم کردن دسترسی از یک IP مشخص توسط کارفرما باشد.

۴,۵. **اطلاع‌رسانی تغییرات:** هرگونه تغییر اساسی در زیرساخت شبکه، افزودن یا حذف تجهیزات، یا تغییرات مهم در پیکربندی که ممکن است بر دامنه یا نتایج ارزیابی تأثیر بگذارد، باید بلافاصله به مجری اطلاع داده شود.

۴,۶. **پرداخت به موقع تعهدات مالی:** پرداخت مبالغ قرارداد طبق زمان‌بندی مندرج در ماده ۴.

ماده ۵: مبلغ قرارداد، شرایط پرداخت و تضمین‌ها

۵,۱. **مبلغ کل قرارداد:** کل مبلغ این قرارداد مبلغ [مبلغ به عدد] [واحد پول] (به حروف: [مبلغ به حروف]) تعیین می‌گردد. این مبلغ شامل کلیه هزینه‌های مربوط به اجرای خدمات ارزیابی، تهیه گزارش، ارائه پیشنهادات، جلسات هماهنگی و ارائه، و دوره تضمین اولیه پس از تحویل گزارش نهایی می‌باشد.

۵,۲. **ساختار پرداخت:** نحوه پرداخت به شرح زیر خواهد بود:

الف) **پیش‌پرداخت:** [درصد]٪ از مبلغ کل قرارداد، معادل [مبلغ پیش‌پرداخت] [واحد پول]، به عنوان پیش‌پرداخت، پس از امضای قرارداد و پیش از شروع عملیات اجرایی، توسط کارفرما به مجری پرداخت خواهد شد.

ب) **پرداخت میانی (در صورت وجود):** در قراردادهای بلندمدت یا پروژه‌های فازبندی شده، ممکن است پرداخت‌های میانی بر اساس پیشرفت فیزیکی یا تکمیل فازهای مشخص (مثلاً پس از اتمام مرحله شناسایی و اسکن) تعیین شود. (این بخش در صورت لزوم فعال و جزئیات آن در پیوست قرارداد ذکر خواهد شد).

ج) **پرداخت نهایی:** [درصد]٪ باقی‌مانده از مبلغ کل قرارداد، معادل [مبلغ نهایی] [واحد پول]، پس از تحویل نهایی گزارش جامع و مورد تأیید کارفرما، و در پایان دوره تضمین اولیه (موضوع ماده ۹)، توسط کارفرما به مجری پرداخت خواهد شد.

۵,۳. **مستندات پرداخت:** کلیه پرداخت‌ها منوط به ارائه صورت‌وضعیت کتبی و مورد تأیید از سوی مجری و دریافت فاکتور رسمی (در صورت لزوم) خواهد بود.

۵,۴. **تضمین حسن انجام کار:** مجری متعهد می‌گردد به منظور تضمین حسن انجام تعهدات خود، [مبلغ یا درصدی] از کل مبلغ قرارداد را تا [مدت زمان] پس از تسویه نهایی، به صورت [وثیقه نقدی/تضمین بانکی/سفته] نزد کارفرما تودیع نماید. این تضمین پس از اتمام موفقیت‌آمیز دوره تضمین و رفع کلیه موارد احتمالی، مسترد خواهد شد.

ماده ۶: مدت قرارداد و زمان‌بندی اجرایی

۶,۱. **مدت کل قرارداد:** مدت زمان اجرای این قرارداد از تاریخ امضای طرفین، معادل [تعداد] روز کاری/هفته/ماه شمسی تعیین می‌گردد.

۶,۲. **شروع عملیات:** عملیات اجرایی ارزیابی از تاریخ [تاریخ دقیق شروع] آغاز خواهد شد.

۶,۳. **برنامه زمان‌بندی تفصیلی (Time Schedule):** برنامه زمان‌بندی تفصیلی اجرای مراحل مختلف قرارداد، شامل زمان‌بندی دقیق برای هر یک از فازهای شناسایی، تحلیل، تست نفوذ، تهیه گزارش، و ارائه، در **پیوست ب** (Project Schedule) این قرارداد که جزئی جدایی‌ناپذیر از آن است، ارائه خواهد شد. کلیه طرفین موظف به رعایت زمان‌بندی تعیین شده هستند.

۶,۴. **تأخیرات:** در صورت بروز هرگونه تأخیر که ناشی از قصور یا قصور طرف دیگر نباشد (مانند فورس ماژور)، مدت قرارداد به تناسب قابل تمدید خواهد بود، مشروط بر آنکه طرف متأثر، حداکثر ظرف مدت [تعداد] روز کاری از وقوع‌آن، مراتب را به صورت کتبی به طرف دیگر اعلام نماید.

ماده ۷: محرمانگی و امنیت اطلاعات (NDA)

۷,۱. **تعهد محرمانگی:** کلیه اطلاعات، مستندات، یافته‌های فنی، اسرار تجاری، داده‌های مشتریان، و هرگونه اطلاعات دیگری که طرفین در طول اجرای این قرارداد به صورت مستقیم یا غیرمستقیم از طرف مقابل دریافت می‌نمایند یا به آن‌ها دسترسی پیدا می‌کنند (اعم از اطلاعات فنی، مالی، عملیاتی، یا استراتژیک)، «اطلاعات محرمانه» تلقی می‌شود.

۷,۲. **محدودیت استفاده:** هر یک از طرفین متعهد می‌گردد که اطلاعات محرمانه طرف دیگر را صرفاً به منظور اجرای این قرارداد به کار گیرد و تحت هیچ شرایطی، بدون کسب رضایت کتبی صریح و پیشین طرف دیگر، آن را افشا، منتشر، یا در اختیار اشخاص ثالث (اعم از حقیقی یا حقوقی) قرار ندهد. استثناء موارد قانونی الزام‌آور (مانند دستور مراجع قضایی) که باید مراتب آن بلافاصله به طرف دیگر اطلاع داده شود.

۷,۳. **تدابیر امنیتی:** مجری متعهد می‌گردد در خصوص حفاظت از اطلاعات کارفرما، تدابیر امنیتی فنی و سازمانی لازم را اتخاذ نماید، از جمله:

الف) محدود کردن دسترسی به اطلاعات محرمانه صرفاً برای اعضای تیم ارزیابی که به صورت مستقیم در پروژه دخیل هستند و نیاز به اطلاع از آن اطلاعات دارند.

ب) آموزش تیم ارزیابی در خصوص اهمیت محرمانگی و خطرات ناشی از افشای اطلاعات.

ج) استفاده از ابزارها و روش‌های امن برای ذخیره‌سازی و انتقال اطلاعات (مانند رمزنگاری).

د) اطمینان از امحاء امن اطلاعات در پایان قرارداد یا در صورت تقاضای کارفرما.

۷,۴. **حفاظت از گزارش:** گزارش نهایی تهیه شده توسط مجری، به عنوان اطلاعات محرمانه کارفرما تلقی شده و مجری حق استفاده، انتشار، یا افشای آن به صورت کلی یا جزئی، بدون کسب اجازه کتبی از کارفرما را ندارد.

۷,۵. **مدت تعهد:** تعهدات محرمانگی مقرر در این ماده، پس از اتمام یا فسخ قرارداد، برای مدت [تعداد] سال (یا به صورت دائمی، بسته به ماهیت اطلاعات) همچنان لازم‌الاجرا خواهد بود.

ماده ۸: مالکیت معنوی، داده‌ها و نتایج

۸,۱. **مالکیت نتایج:** کلیه حقوق مالکیت معنوی ناشی از خدمات ارزیابی، یافته‌های فنی، گزارش‌ها، مستندات، و هرگونه خروجی ملموس یا ناملموس دیگر که در نتیجه اجرای این قرارداد توسط مجری تولید می‌شود، پس از تسویه کامل مبلغ قرارداد و مفاد ماده ۴، به صورت کامل به کارفرما منتقل می‌گردد.

۸,۲. **استفاده مجری از نتایج:** مجری حق دارد از دانش فنی کسب شده، متدولوژی‌ها، و یافته‌های عمومی (که به هیچ وجه قابل انتساب به کارفرما و شناسایی‌کننده اطلاعات محرمانه وی نباشد) جهت بهبود خدمات خود و آموزش پرسنل، با رعایت کامل تعهدات محرمانگی این قرارداد، استفاده نماید.

۸,۳. **داده‌های کارفرما:** کلیه داده‌ها، اطلاعات، و دارایی‌های متعلق به کارفرما که در طول فرآیند ارزیابی توسط مجری مورد استفاده یا پردازش قرار می‌گیرند، همچنان متعلق به کارفرما باقی مانده و مجری هیچ‌گونه حقی بر آن‌ها نخواهد داشت. مجری متعهد به استرداد یا امحاء امن کلیه داده‌های کارفرما در پایان قرارداد است.

ماده ۹: دوره تضمین، رفع اشکال و پشتیبانی

۹,۱. **دوره تضمین:** پس از تحویل رسمی گزارش جامع نهایی توسط مجری و تأیید دریافت آن توسط کارفرما، دوره‌ای به مدت [تعداد] روز کاری (دوره تضمین) آغاز می‌گردد. در طول این دوره، مجری متعهد به ارائه پشتیبانی لازم جهت رفع اشکالات احتمالی گزارش و پاسخگویی به سوالات تکمیلی کارفرما می‌باشد.

۹,۲. فرآیند رفع اشکال:

الف) **گزارش موارد اشکال:** در صورتی که کارفرما در طول دوره تضمین، موارد اشکال، ابهام، یا خطای فنی در گزارش را شناسایی نماید (مانند: یافتن یک آسیب‌پذیری که در گزارش ذکر نشده، عدم صحت یک یافته گزارش شده، ابهام در تشریح فنی یک مورد، یا عدم کارایی یک پیشنهاد اصلاحی)، باید مراتب را به صورت کتبی و با جزئیات کامل (شامل شرح مورد، مستندات، و ارجاع به بخش مربوطه در گزارش) به مجری اعلام نماید.

ب) **بررسی مجدد توسط مجری:** مجری موظف است حداکثر ظرف مدت [تعداد] روز کاری از دریافت گزارش اشکال از سوی کارفرما، نسبت به بررسی دقیق موارد مطروحه اقدام نماید.

ج) **تأیید و اصلاح:** در صورتی که اشکال یا خطای گزارش شده توسط کارفرما تأیید گردد، مجری متعهد است نسبت به اصلاح گزارش، ارائه توضیحات تکمیلی، یا انجام بررسی مجدد جزئی (در صورت لزوم) اقدام نماید. این اصلاحات باید به صورت مستند و جزئی به کارفرما ارائه گردد.

د) **عدم تأیید مجری:** در صورتی که پس از بررسی، مجری تشخیص دهد که مورد اعلام شده از سوی کارفرما، اشکال یا خطای فنی نبوده است (مثلاً ناشی از درک نادرست یا تغییرات در محیط کارفرما پس از ارزیابی)، باید دلایل عدم تأیید خود را به صورت مستند و فنی به کارفرما اعلام نماید. در این صورت، طرفین می‌توانند در خصوص انجام بررسی‌های بیشتر یا ارجاع به داوری تصمیم‌گیری نمایند.

۹,۳. پشتیبانی فنی تکمیلی (خارج از دوره تضمین): پس از اتمام دوره تضمین، کارفرما می‌تواند در صورت نیاز، نسبت به انعقاد قرارداد پشتیبانی فنی مجزا یا درخواست خدمات تکمیلی (مانند ارزیابی مجدد پس از اعمال اصلاحات) با مجری اقدام نماید. شرایط این خدمات در قراردادهای جداگانه تعیین خواهد شد.

ماده ۱۰: مسئولیت‌ها، محدودیت‌ها و فسخ قرارداد

۱۰,۱. مسئولیت مجری:

الف) **تعهد به دقت و صداقت:** مجری متعهد است ارزیابی را با نهایت دقت، صداقت حرفه‌ای، و بر اساس بهترین شیوه‌ها و استانداردهای شناخته شده انجام دهد.

ب) **محدودیت تضمین کشف ٪۱۰۰:** با توجه به ماهیت پویا و پیچیده حملات سایبری و شبکه‌ها، هیچ تضمینی مبنی بر کشف قطعی و ٪۱۰۰ کلیه آسیب‌پذیری‌های موجود وجود ندارد. هدف این قرارداد، کاهش قابل توجه ریسک از طریق شناسایی بخش عمده‌ای از آسیب‌پذیری‌های مهم و رایج است.

ج) **مسئولیت خسارات مستقیم:** مجری تنها در قبال خسارات مستقیم وارده به شبکه و دارایی‌های کارفرما که ناشی از قصور عمدی (Intentional Misconduct) یا بی‌احتیاطی شدید (Gross Negligence) تیم ارزیابی در اجرای تست‌ها باشد، و این قصور به طور مستند اثبات شود، مسئولیت خواهد داشت. خسارات غیرمستقیم، تبعی، یا از دست رفتن سود، خارج از تعهدات مجری است.

د) **جبران خسارت:** سقف مسئولیت مجری در قبال هرگونه خسارت وارده، حداکثر معادل کل مبلغ قرارداد خواهد بود.

۱۰,۲. مسئولیت کارفرما:

الف) **تأیید و استفاده از گزارش:** کارفرما مسئولیت نهایی بررسی، تأیید، و اجرای پیشنهادات ارائه شده در گزارش را بر عهده دارد. مجری هیچ‌گونه مسئولیتی در قبال عدم اجرای پیشنهادات یا اجرای نادرست آن‌ها توسط کارفرما نخواهد داشت.

ب) **حفظ امنیت پس از ارزیابی:** مسئولیت حفظ امنیت شبکه پس از اتمام ارزیابی و اجرای اصلاحات، بر عهده کارفرما است.

۱۰,۳. شرایط فسخ قرارداد:

الف) **توافق طرفین:** این قرارداد در هر زمان با توافق کتبی طرفین قابل فسخ است.

ب) **تخلف از مفاد:** در صورت نقض اساسی هر یک از تعهدات این قرارداد توسط یکی از طرفین (مانند نقض محرمانگی، عدم پرداخت مطالبات، عدم همکاری مؤثر)، طرف دیگر می‌تواند پس از اخطار کتبی ۱۰ روزه و عدم رفع تخلف در این مدت، قرارداد را فسخ نماید.

ج) **فورس ماژور:** در صورت بروز حوادث قهریه (مانند زلزله، سیل، جنگ، اعتصابات عمومی) که ادامه قرارداد را برای یکی از طرفین غیرممکن سازد، قرارداد قابل فسخ خواهد بود.

د) **پیامدهای فسخ:** در صورت فسخ، هزینه‌های انجام شده تا زمان فسخ بر اساس صورت‌وضعیت تأیید شده توسط مجری، توسط کارفرما پرداخت خواهد شد. در صورت فسخ از سوی کارفرما بدون دلیل موجه، کارفرما موظف به پرداخت درصدی از کل قرارداد به عنوان خسارت (مثلاً [درصد]٪) خواهد بود. در صورت فسخ از سوی مجری بدون دلیل موجه، مجری موظف به استرداد مبلغ پیش‌پرداخت و پرداخت خسارتی مشابه خواهد بود.

ماده ۱۱: حل اختلاف و قوانین حاکم

طرفین توافق نمودند کلیه اختلافات و دعاوی ناشی از این قرارداد یا راجع به آن از جمله انعقاد، اعتبار، فسخ، تفسیر یا اجرای آن، از طریق داوری یکی از داوران عضو سامانه جامع داوری ایران با تعیین و نصب داور همچنین تعیین حق الزحمه داوری از سوی آن

سامانه، بعنوان مقام ناصب حل و فصل گردد لذا پس از ثبت درخواست در سامانه مذکور، داور منصوب به موضوع اختلاف رسیدگی و رای لازم را صادر می نماید. شرط داوری حاضر، موافقتنامه‌ای مستقل از قرارداد اصلی بوده و لازم‌الاجرا می باشد.

ماده ۱۲: فورس ماژور (حوادث قهریه)

۱۲,۱. هیچ یک از طرفین در قبال تأخیر یا عدم اجرای تعهدات خود (به استثنای تعهدات مالی)، در صورتی که ناشی از حوادث قهریه یا غیرقابل پیش‌بینی و خارج از کنترل متعارف باشد (مانند جنگ، شورش، اعتصابات گسترده، بلایای طبیعی، اقدامات تروریستی، یا مقررات دولتی ناگهانی که مانع اجرای قرارداد شود)، مسئولیتی نخواهند داشت.

۱۲,۲. طرفی که تحت تأثیر فورس ماژور قرار گرفته است، موظف است بلافاصله (حداکثر ظرف مدت [تعداد] روز کاری) مراتب را به صورت کتبی به طرف دیگر اطلاع داده و مستندات لازم را ارائه نماید.

۱۲,۳. در صورت ادامه فورس ماژور برای مدتی بیش از [تعداد] روز کاری، طرفین می‌توانند در خصوص ادامه یا فسخ قرارداد به توافق رسیده و در صورت فسخ، تسویه حساب بر اساس مفاد ماده ۱۰ انجام خواهد شد.

ماده ۱۳: سایر مقررات

۱۳,۱. **پیوست‌ها:** کلیه پیوست‌های این قرارداد (شامل پیوست الف: دامنه خدمات و محدودیت‌ها، پیوست ب: برنامه زمان‌بندی، و سایر پیوست‌های احتمالی) جزئی جدایی‌ناپذیر از این قرارداد محسوب شده و از اعتبار یکسان برخوردارند.

۱۳,۲. **اصلاحات:** هرگونه تغییر، اصلاح، یا الحاق به مفاد این قرارداد، تنها در صورتی معتبر خواهد بود که به صورت کتبی بوده و به امضای نمایندگان مجاز طرفین برسد.

۱۳,۳. **قوه قهریه بندها:** در صورتی که هر یک از بندهای این قرارداد توسط مراجع ذی‌صلاح غیرقانونی، باطل، یا غیرقابل اجرا تشخیص داده شود، سایر بندها همچنان معتبر و لازم‌الاجرا باقی خواهند ماند.

۱۳,۴. **عدم اسقاط حقوق:** عدم استفاده یا تأخیر در استفاده از هر یک از حقوق مقرر در این قرارداد توسط هر یک از طرفین، به منزله اسقاط آن حق تلقی نخواهد شد.

ماده ۱۴: امضاء و اعتبار قرارداد

این قرارداد در ۱۴ ماده و [تعداد] تبصره (در صورت وجود)، در دو نسخه متحدالمتن و با اعتبار واحد، در تاریخ فوق‌الذکر تنظیم، امضاء و مبادله گردید و از تاریخ امضاء برای طرفین لازم‌الاجرا است.

امضاءها:

از طرف کارفرما:

نام و نام خانوادگی:

سمت:

امضاء:

مهر شرکت (در صورت وجود):

تاریخ:

از طرف مجری:

نام و نام خانوادگی:

سمت:

امضاء:

مهر شرکت (در صورت وجود):

تاریخ: