توافق‌نامه سطح خدمات Padvish MDR

شرکت نرم افزاری امن پرداز

شرکت نرم افزاری
امن‌پرداز

سطح محرمانگی: عادی

نسخه ۱.۳
بهار ۱۴۰۴

فهرست مطالب

۱. مقدمه

این سند توافق‌نامه سطح خدمات مرکز کشف نفوذ و مقابله با تهدیدات پیشرفته Padvish MDR را بیان می‌کند که شامل تعهدات خدمات و شرایط آن می‌باشد. در سرتاسر این سند، از لفظ «امن‌پرداز» به عنوان ارائه‌دهنده خدمات Padvish MDR و از لفظ «بهره‌بردار» به عنوان کارفرما/مشتری/استفاده‌کننده از خدمات فوق استفاده شده است.

مطالب این سند بخش اصلی اسناد قانونی فی‌مابین بهره‌بردار و امن‌پرداز را تشکیل می‌دهد و مکمل و جایگزین هر نوع تعهد مربوط به سطح خدمات Padvish MDR می‌باشد که در سایر اسناد مکتوب یا غیرمکتوب فی‌مابین دو طرف ردوبدل شده است. در صورت بروز هرگونه تناقض بین محتوای این سند با سایر اسناد مکتوب، تعهدات مندرج در این سند نافذ و جایگزین خواهد بود.

بهره‌بردار می‌پذیرد و موافقت می‌کند که امن‌پرداز ممکن است هر از چندگاهی بدون کاهش یا تضعیف عملکرد کلی خدمات خود، تغییراتی در آن بدهد، و نیز امن‌پرداز می‌تواند محتویات این سند را جهت تطبیق با واقعیت خدمات ارائه شده اصلاح یا بروزرسانی نماید.

۲. تعاریف و اصطلاحات

رج	اصطلاح	شرح
۱.	امن‌پرداز	شرکت نرم‌افزاری امن‌پرداز که ارائه دهنده خدمات Padvish MDR می‌باشد
۲.	بهره‌بردار	مشتری/کارفرما یا هر شخصی که خدمات Padvish MDR را خریداری کرده و لایسنس مربوطه را دریافت و قصد دارد در شبکه خود استفاده نماید
۳.	رابط بهره‌بردار	فرد یا افرادی که از سمت *بهره‌بردار* به *امن‌پرداز* جهت انجام هماهنگی‌های لازم معرفی می‌شود. این فرد/افراد باید دانش فنی و اختیارات لازم جهت فهم هشدارها و در دسترس قرار دادن فوری سیستم‌ها جهت بررسی و رفع مشکلات را داشته باشند، و همواره نیز در دسترس باشند.
۴.	خدمات	در این سند مقصود از کلمه خدمات به تنهایی، یا خدمات Padvish MDR خدمات مرکز کشف نفوذ و مقابله با تهدیدات پیشرفته Padvish MDR می‌باشد.
۵.	طول دوره خدمات	حدفاصل بین تاریخ شروع *خدمات* تا پایان آن که توسط *بهره‌بردار* خریداری شده است.
۶.	هشدار	نفوذ تایید شده یا احتمال نفوذ به سیستم‌ها که تهدیدی برای امنیت دارایی‌های بهره‌بردار محسوب می‌شود.
۷.	سطح (حساسیت) هشدار	سطح هشدار یا سطح حساسیت هشدار، نشان‌دهنده میزان فوریت و نحوه برخورد با آن می‌باشد و در بند ۲.۳ در سند تشریح شده است.
۸.	هشدارهای فوری	هشدارهای با سطح حساسیت قرمز و یا سیاه
۹.	پاسخ به رخداد	عملیات بررسی وجود نفوذ، کشف اثرات و رفع آنها که با تماس با رابط بهره‌بردار و سپس اخذ دسترسی آغاز می‌شود. (اطلاعات بیشتر در بند ۳.۳)
۱۰.	سلامت سیستم	مجموعه عواملی که در عملکرد صحیح سیستم و امکان محافظت از آن موثر هستند: از قبیل صحت نصب و عملکرد ایجنت گرفته تا نصب

		وصله‌های امنیتی سیستم‌عامل و نرم‌افزارها و مانند آن. (اطلاعات بیشتر در بند ۳.۲)
۱۱.	تیم پاسخ به رخداد	مقصود از تیم پاسخ به رخداد در این سند، تیمی از *امن‌پرداز* است که وظیفه نظارت، بررسی و پاسخ به رخدادهای امنیتی را دارد.
۱۲.	ادعا	اعلام درخواست از سمت *بهره‌بردار* که تعهدات مندرج در این توافق‌نامه نقض شده و تقاضای اعتبار خدمات مطابق بند ۴
۱۳.	لایسنس	مجوز نصب و استفاده از خدمات Padvish MDR که از سمت *امن‌پرداز* برای استفاده در شبکه *بهره‌بردار* صادر شده و دارای ویژگی‌های مشخص مانند تاریخ شروع و پایان، تعداد ایجنت، و... می‌باشد.
۱۴.	ایجنت (پادویش)	مقصود از کلمه ایجنت یا ایجنت پادویش در این سند، نسخه‌ای از آنتی‌ویروس پادویش است که با لایسنس مرتبط با MDR و تحت مدیریت مرکزی فعال شده باشد.
۱۵.	سرور مدیریت مرکزی پادویش	که به نام Padvish Management Server یا PMS نیز خوانده می‌شود، یک سرویس مرکزی مستقر در شبکه *بهره‌بردار* می‌باشد که مدیریت ایجنت‌های آنتی‌ویروس پادویش از طریق آن انجام می‌شود.
۱۶.	مولفه‌های Padvish EDR	مولفه‌های محصول Padvish EDR که شامل انواع ماژول‌های سنسورها، داشبوردها، شکار تهدیدات، و ... می‌شود. (مطابق مستندات آن)
۱۷.	سامانه مرکزی Padvish MDR	سرور مرکزی سامانه MDR که در محل امن‌پرداز وجود دارد و وظیفه جمع‌آوری، پردازش و کنترل این خدمات را برعهده دارد.
۱۸.	دستگاه‌های تحت محافظت	مجموعه دستگاه‌هایی که *بهره‌بردار* قصد حفاظت از آنها توسط *خدمات Padvish MDR* را دارد، ایجنت پادویش روی آنها نصب بوده و با لایسنس مرتبط فعال و متصل به سامانه‌های مدیریتی و MDR هستند.

۲/۱. سطوح خدمات

خدمات Padvish MDR شامل دو سطح زیر می‌گردد که توسط بهره‌بردار در زمان خرید قابل انتخاب می‌باشد و با لایسنس از یکدیگر تفکیک می‌شوند:

- **سطح بهینه:** در این سند مقصود از «سطح بهینه» مجوز Padvish MDR Optimum می‌باشد و شامل خدمات پایه‌ای Padvish MDR به صورت ابری است. در این سطح، احتیاجی به نصب *مولفه‌های Padvish EDR* در شبکه نبوده و از همان *سرور مدیریت مرکزی پادویش* جهت جمع‌آوری و ارسال اطلاعات به *سامانه مرکزی Padvish MDR* استفاده می‌شود. این سطح عمق سنسور کمتری داشته و فاقد کنسول وب در اختیار *بهره‌بردار* است.
- **سطح پیشرفته:** در این سند مقصود از «سطح پیشرفته» مجوز Padvish MDR Base/Select/Expert می‌باشد و شامل خدمات پیشرفته Padvish MDR است که بر روی محصول Padvish EDR بنا می‌شود و لذا دارای کنسول و رابط کاملی در سمت بهره‌بردار و عمق سنسور کاملی نیز دارد.

۲/۱/۱. مقایسه سطوح خدمات

رج	قابلیت	سطح بهینه	سطح پیشرفته
۱.	نظارت ۷ در ۲۴	✓	✓
۲.	تیم متخصص با تجربه بررسی حملات سایبری اخیر کشور	✓	✓
۳.	عمق سنسورهای پیشرفته	متوسط	عمیق
۴.	اعلام هشدارهای امنیتی	✓	✓
۵.	اعلام هشدار از طریق پیامک/تماس	✓	✓
۶.	اعلام هشدارهای مهم به صورت کتبی	✓	✓
۷.	شکار تهدیدات فعال	✓	✓
۸.	سطح سرویس تضمین شده	✓	✓
۹.	نگهداری هشدارها تا یکسال	✓	✓
۱۰.	گزارش دوره‌ای وضعیت شبکه	✓	✓
۱۱.	عملیات فارنزیک تا سقف ساعت مشخص	✓	✓
۱۲.	ارزیابی وضعیت امنیتی شبکه	–	✓
۱۳.	اعلام نقاط ضعف و قابل بهبود شبکه	–	✓
۱۴.	نگهداری لاگ‌های خام به مدت تعیین شده توسط سیاست سازمان	–	✓
۱۵.	دسترسی به سامانه وب Padvish EDR	–	✓

۲/۲. مولفه‌های Padvish MDR

جهت راه‌اندازی خدمت Padvish MDR در یک شبکه، باید مولفه‌های زیر در آن شبکه راه‌اندازی شوند:

۱. **ایجنت پادویش**: نسخه‌ای به‌روز از *آنتی‌ویروس پادویش* که بر روی *دستگاه‌های تحت محافظت*، با لایسنس Padvish MDR مناسب تحت *سرور مدیریتی پادویش* فعال شده باشد و مکانیزم‌های محافظتی آن (مطابق دستورالعمل‌ها و توصیه‌های امنیتی تولیدکننده) به طور کامل فعال باشند. (عملکرد صحیح ایجنت ممکن است منوط به ریست سیستم پس از نصب یا آپگرید آن باشد)

۲. **سرور مدیریتی پادویش**: نسخه‌ای به‌روز از سرویس مدیریتی پادویش که بر روی یک یا چند سرور به صورت مستر/اسلیو درون شبکه *بهره‌بردار* نصب می‌شود و هر سرور، وظیفه مدیریت *ایجنت‌های پادویش* در محدوده خود را داراست. تمامی *سرورهای مدیریتی پادویش* – علاوه بر نیازمندی‌های

ارتباطی معمول خود که در سند نیازمندی‌های نصب به آن اشاره شده – باید با *سامانه مرکزی Padvish MDR* اتصال بدون محدودیت داشته باشند.

۳. **مجموعه سرورهای EDR پادویش: (اختصاصی سطح پیشرفته)** نسخه‌ای به‌روز از مجموعه کامل *مولفه‌های Padvish EDR* که درون شبکه بهره‌بردار نصب بوده و *ایجنت‌های پادویش* و *سرور(های) مدیریتی* پادویش اطلاعات خود را به آنها ارسال می‌کنند. این سرورها نیز – علاوه بر نیازمندی‌های ارتباطی معمول خود که در سند نیازمندی‌های نصب محصول Padvish EDR به آن اشاره شده – باید اتصال بدون محدودیت با *سامانه مرکزی Padvish MDR* داشته باشند.

۲٫۳. سطوح حساسیت هشدارهای امنیتی

در مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR) هشدارهای امنیتی از نظر درجه خطر و اهمیت به سطوح مختلفی تقسیم‌بندی می‌شوند که با رنگ هشدار مشخص می‌شود:

۱. **هشدار سیاه (بررسی فوری)**: خطر فوری و قطعی هک و نفوذ

۲. **هشدار قرمز (تماس فوری)**: احتمال جدی هک و نفوذ که باید فورا بررسی شود

۳. **هشدار نارنجی (غیرفوری)**: موارد حائز اهمیت بدون فوریت

هر سطح حساسیت هشدار با توجه به درجه اهمیت و فوریت خود، از یک SLA جداگانه برخوردار می‌باشد.

۳. محدوده خدمات

۳/۱. مرحله راه‌اندازی

در مرحله راه‌اندازی خدمات، بهره‌بردار باید عملیات زیر را انجام دهد:

۱. **معرفی رابط**: فرد یا تیم *رابط بهره‌بردار* را جهت برقراری تماس در *طول دوره خدمات* معرفی کرده و شماره تلفن همراه، ثابت، و ایمیل مربوطه را در اختیار *تیم پاسخ به رخداد* قرار دهد. *رابط بهره‌بردار* باید به صورت ۲۴×۷ جهت دریافت تماس‌های اضطراری در دسترس بوده و احاطه فنی مناسب و اختیارات لازم جهت فراهم کردن شرایط بررسی فوری دستگاه‌های در خطر را داشته باشد.

۲. **نصب و فعالسازی کلیه مولفه‌های Padvish MDR**: *بهره‌بردار* باید کلیه مولفه‌های Padvish MDR که در بخش ۰ بیان شد را به طرز صحیح و کامل در شبکه تحت حفاظت خود نصب، فعالسازی و پیکربندی نموده و از عملکرد آنها اطمینان حاصل نماید.

۳. **اطمینان از اتصال با *سامانه مرکزی Padvish MDR***: *بهره‌بردار* باید چنانکه در بخش ۰ بیان شد، ارتباط مستقیم *سرور(های) مدیریتی پادویش* (در خصوص **سطح بهینه** و **سطح پیشرفته**) و *مولفه‌های Padvish EDR* (در خصوص **سطح پیشرفته**) را با *سامانه مرکزی Padvish MDR* برقرار نموده و تست نماید.

۳/۲. بررسی دوره‌ای سلامت سیستم

۱. سلامت سیستم، شامل مجموعه‌ای از عوامل به شرح زیر است:

a. وجود پیکربندی صحیح،

b. فعال بودن کامل محافظت‌ها،

c. متصل بودن ایجنت‌ها به سرورهای مدیریتی پادویش

d. (در مورد **سطح پیشرفته**) متصل بودن ایجنت‌ها به سرورهای Padvish EDR،

e. متصل بودن سرورهای مدیریتی پادویش به سامانه مرکزی Padvish MDR

f. (در مورد **سطح پیشرفته**) متصل بودن سرورهای Padvish EDR به سامانه مرکزی Padvish MDR،

g. به‌روز بودن سیستم‌عامل و نرم‌افزارهای شخص ثالث،

h. صحت و سینک بودن تاریخ سیستم

i. به‌روز بودن پایگاه امضا، و نیز نسخه ایجنت و سایر مولفه‌های Padvish MDR،

j. عدم وجود اکانت‌ها با پسوردهای ضعیف، قابل حدس، یا مشابه،

k. وجود پشتیبان به‌روز و کامل از داده‌ها،

l. عدم وجود هشدار امنیتی بر روی سیستم‌ها

m. و به طور کلی رعایت نکات امنیتی استاندارد و معقول

۲. *بهره‌بردار* باید به صورت دوره‌های حداقل هفتگی، وضعیت سلامت سیستم‌ها را بررسی نموده و اقدامات لازم مانند آپدیت کردن، بکاپ گرفتن، اعمال کردن سیاست‌های امنیتی و... را جهت رفع نواقص انجام دهد. در صورتیکه اقدامات لازم جهت رفع موضوع توسط *بهره‌بردار* انجام نگیرد، کاهش توانایی خدمات در تشخیص تهدیدات امنیتی که در اثر این موضوع ایجاد شود به عهده بهره‌بردار خواهد بود.

۳. **(اختصاصی سطح پیشرفته)** تیم پاسخ به رخداد امن‌پرداز موارد زیر از سلامت سیستم را بررسی نموده و در صورت نقض موارد امنیتی به صورت هشدار اعلام می‌کند. وظیفه رفع موارد اعلامی با *بهره‌بردار* خواهد بود:

a. متصل بودن سرورهای مدیریتی پادویش به سامانه مرکزی Padvish MDR

b. متصل بودن سرورهای Padvish EDR به سامانه مرکزی Padvish MDR،

c. خاموش شدن کامل یک محافظت: این مورد فقط ناظر به تغییرات جدید بوده و تنظیماتی که قبل یا حین مرحله راه‌اندازی انجام شده باشد را شامل نمی‌شود. این مورد شامل خاموش بودن بخشی از یک محافظت یا پیکربندی اشتباه آن نمی‌شود.

۳/۳. کشف، بررسی و پاسخ به رخداد

تیم پاسخ به رخداد امن‌پرداز موارد زیر را برای کشف، بررسی و پاسخ به رخدادهای امنیتی انجام می‌دهد:

۱. **پردازش:** اطلاعات تشخیص‌ها و سنسورها پردازش می‌شوند تا موارد مهم و نشانه‌های تهدید از آنها استخراج شده و سیستم برای تشخیص خودکار هشدار تنظیم گردد.

۲. **پاسخ به رخداد:** *تیم پاسخ به رخداد* در صورت مواجهه با موارد مشکوک و حساس، از طرق اعلام شده در *مرحله راه‌اندازی* با *رابط بهره‌بردار* تماس گرفته و هشدار را اعلام می‌نماید. پس از اعلام، وظیفه دادن دسترسی به سیستم(ها) جهت عملیات فارنزیک توسط *تیم پاسخ به رخداد امن‌پرداز* با *رابط بهره‌بردار* خواهد بود.

۳. **عملیات فارنزیک:** عملیات فارنزیک برای اطمینان از صحت *هشدارها* انجام می‌گیرد، و شامل اخذ دسترسی به یک سیستم و بررسی تهدیدات و شواهد موجود در آن برای یافتن و تکمیل اطلاعات *پرونده* و یا پاسخ به رخداد امنیتی بهره گرفته می‌شود. *تیم پاسخ به رخداد*، ممکن است از نتایج عملیات فارنزیک برای استثنا کردن رویدادهای معمول شبکه استفاده کند تا موارد مشکوک و غیرعادی بهتر دیده شوند.

مهم: *بهره‌بردار* می‌پذیرد که موافقت وی برای بررسی سیستم‌ها توسط *امن‌پرداز* و اصلاح پیکربندی‌ها یا اجرای ابزارهای ردیابی ممکن است منجر به قطعی یا تاثیر بر عملیات و خدمات موجود در سیستم‌های وی گردد. به علاوه *بهره‌بردار* می‌پذیرد که عدم موافقت برای بررسی سیستم‌ها یا ایجاد تغییرات می‌تواند منجر به فعالیت مخرب جدید یا بدتر شدن وضعیت امنیتی گردد. اگر *بهره‌بردار* درخواست *امن‌پرداز* را برای بررسی یا انجام تغییرات رد نموده یا در آن تاخیر ایجاد نماید، *امن‌پرداز* هیچ تعهدی برای هیچگونه خسارتی که در اثر عملیات مخرب ایجاد می‌شود نخواهد داشت.

۳/۴. زمان واکنش

زمان واکنش، به مدت زمانی اشاره دارد که از لحظه *تعیین حساسیت هشدار* آغاز شده و در لحظه اولین تماس با *رابط بهره‌بردار* (از طریق ایمیل، پیامک، یا تلفن) پایان می‌یابد.

حداکثر *زمان واکنش* در مورد انواع *سطوح حساسیت هشدار* به شرح جدول زیر می‌باشد:

سطح حساسیت هشدار	زمان واکنش (از لحظه تعیین حساسیت هشدار)
فوری (قرمز/سیاه)	۳۰ دقیقه
غیرفوری (نارنجی)	ساعات اداری (۷ صبح تا ۷ شب روزهای کاری)

امن‌پرداز متعهد می‌شود که در خصوص هشدارهای با *سطح حساسیت* فوری (قرمز/سیاه)، زمان واکنش حداکثر ۳۰ دقیقه باشد. در صورتیکه *امن‌پرداز* موفق نشود این تعهد را برآورده کند، *بهره‌بردار* می‌تواند مطابق بند ۴ وارد فرایند *اعلام ادعا* و دریافت اعتبار گردد.

۳/۵. دسترس‌پذیری

تمامی عملیات کشف، بررسی و پاسخ به رخداد (بند ۳.۳) توسط *تیم پاسخ به رخداد امن‌پرداز* به صورت ۲۴×۷×۳۶۵ انجام می‌گیرند. به علاوه بهره‌بردار می‌تواند با *تیم پاسخ به* رخداد به صورت ۲۴×۷×۳۶۵ جهت بررسی موارد مشکوک تماس حاصل نماید.

۳/۶. شکار تهدیدات

تیم پاسخ به رخداد امن‌پرداز به صورت فعال نشانه‌های تهدیداتی که از کنترل‌های تشخیص موجود گذشته باشند را جستجو می‌کند. این جستجو در اطلاعاتی انجام می‌شود که توسط سنسورها از روی *دستگاه‌های تحت محافظت* جمع‌آوری شده‌اند و بر اساس تشخیص رفتارها یا تاکتیک‌های مشابهی که قبلا توسط نفوذگران استفاده شده‌اند یا روش‌های ابداعی جدید انجام می‌گیرد. در صورت کشف رفتار مشکوک، با توجه به سطح حساسیت هشدار، فرایند پاسخ به رخداد (بند ۳.۳) انجام خواهد گرفت.

۳/۷. گزارش‌دهی دوره‌ای

امن‌پرداز به صورت دوره‌های ماهانه یا فصلی، گزارشی از تشخیص‌ها، هشدارها، اقدامات انجام شده در پاسخ به رویداد، و توصیه‌های امنیتی جهت بهبود وضعیت امنیت شبکه به *رابط بهره‌بردار* ارسال می‌نماید.

۴. اعلام ادعا و دریافت اعتبار

۴/۱. روش محاسبه اعتبار خدمات

در صورتیکه *امن‌پرداز* نتواند به تعهد خود در خصوص *زمان واکنش* در *هشدارهای* با *سطح حساسیت* فوری عمل نماید، *بهره‌بردار* حق برخورداری از *اعتبار خدمات* مطابق جدول زیر را خواهد داشت:

زمان واکنش	زمان اعتبار / روز
۳۱ تا ۶۰ دقیقه	۱
۶۱ تا ۱۵۰ دقیقه	۳
۱۵۱ تا ۳۰۰ دقیقه	۷
۳۰۱ دقیقه به بالا	۱۵

۱. این اعتبار به پایان مدت لایسنس اضافه خواهد شد.

۲. *بهره‌بردار* در هر روز تقویمی می‌تواند حداکثر یک *ادعا* ثبت نماید.

۴/۲. فرایند اعلام ادعا

۱. به منظور واجد شرایط بودن برای ارائه *ادعا* و دریافت اعتبار، *بهره‌بردار* باید ابتدا با استفاده از رویه‌های تعیین‌شده توسط *امن‌پرداز*، ظرف حداکثر ۱۴ روز تقویمی پس از تاریخ *اعلام هشدار*، پشتیبانی *امن‌پرداز* را از رخداد آن مطلع کند.

۲. برای ارسال یک *ادعا* ، *بهره‌بردار* باید حداکثر ظرف ۱۴ روز تقویمی، ایمیلی با عنوان MDR Credit Claim به آدرس support@amnpardaz.com ارسال نماید و در آن، با مشخص نمودن *هشدار* مورد *ادعا*، مدارک یا مستندات فنی خود را ارائه دهد.

۳. در صورتیکه مدت ثبت *ادعا* توسط *بهره‌بردار* بیش از ۱۴ روز گردد، امکان ثبت و دریافت ادعا منقضی شده تلقی خواهد شد.

٤. *امن‌پرداز* از تمام اطلاعات فنی در دسترس خود برای تأیید *ادعاها* در مورد سطوح خدمات سرویس به صورت منطقی و با حسن نیت استفاده خواهد کرد و ظرف حداکثر ۳۰ روز به درخواست پاسخ خواهد داد. در صورت تایید ادعا، مبلغ اعتبار به دوره بعدی اشتراک *بهره‌بردار* افزوده خواهد شد.

۵. تعهدات بهره‌بردار

بهره‌بردار متعهد می‌شود که وظایف زیر را انجام دهد:

۱. مشخص نمودن یک *رابط بهره‌بردار* که با *تیم پاسخ به رخداد امن‌پرداز* همکاری نماید. *بهره‌بردار* اطمینان حاصل می‌کند که اطلاعات *رابط بهره‌بردار* و اطلاعات تماس نزد *امن‌پرداز* به‌روز و صحیح باشد.

۲. رابط *بهره‌بردار* باید از دانش فنی و اختیارات لازم جهت دادن دسترسی کامل، به موقع و سریع به *تیم پاسخ به رخداد امن‌پرداز* جهت بررسی سیستم‌ها و تجهیزات (روی *دستگاه‌های تحت محافظت* یا غیر آن) در زمان مواجهه با هشدارهای امنیتی برخوردار باشد. به علاوه باید دانش فنی و اختیارات لازم جهت اعمال توصیه‌های امنیتی و پاکسازی تهدیدات و امن‌سازی پیکربندی‌های اعلام شده را داشته باشد.

۳. حصول اطمینان از صحت ارتباطات لازم چنانکه در بخش ۰ گذشت.

۴. حصول اطمینان از صحت نصب و فعال‌سازی، صحت پیکربندی، صحت عملکرد، به‌روز بودن و متصل بودن ایجنت‌های پادویش، سیستم‌عامل و نرم‌افزارها و در یک کلمه بررسی دوره‌ای سلامت سیستم (بند ۳.۲) بر روی دستگاه‌های تحت محافظت

۵. انجام کامل عملیات مرحله راه‌اندازی مطابق بند ۳.۱

۶. حصول اطمینان از عدم وجود فناوری‌ها یا پیکربندی‌هایی که با مسدود کردن ترافیک، حذف لاگ‌ها، یا هر روشی بر کیفیت خدمات اثر بگذارند.

۷. حصول اطمینان از سازگاری با همه قوانین و الزامات سازمانی و ملی خود

۸. رفع تهدیدات و اعمال توصیه‌های امنیتی ارائه شده به بهره‌بردار توسط *امن‌پرداز* و یا اشخاص ثالث در سریعترین زمان ممکن

۹. تهدیداتی که از سمت دستگاه‌ها و تجهیزاتی که جزو *دستگاه‌های تحت محافظت* نیستند (به عنوان مثال همه دستگاه‌هایی که نسخه به‌روز و فعال‌شده با لایسنس مناسب MDR از ایجنت بر روی آنها نصب نیست) ایجاد می‌شوند خارج از حیطه این خدمات و توافق‌نامه می‌باشند و مسئولیت آنها با *بهره‌بردار* می‌باشد.

۱۰. عملیات و اقداماتی که به صراحت در این توافق‌نامه قید نشده‌اند جزئی از خدمات نمی‌باشند و مسئولیت آنها با *بهره‌بردار* می‌باشد. به علاوه *بهره‌بردار* می‌پذیرد که *امن‌پرداز* مسئول تهدیداتی که پیش از تاریخ آغاز خدمات در شبکه وجود داشته‌اند نمی‌باشد.

طبیعتا عدم پایبندی به هر یک از موارد فوق در فرصت لازم، می‌تواند باعث ایجاد تاخیر یا کاهش کیفیت خدمات ارائه شده گردد و در این صورت امن‌پرداز مسئول عواقب چنین تاخیرهایی نخواهد بود.

۶. استثنائات

بهره‌بردار می‌پذیرد که *امن‌پرداز* مسئولیتی در قبال اتفاقات زیر ندارد:

۱. اتفاقاتی که به دلیل تاخیر توسط *بهره‌بردار* در دادن دسترسی جهت عملیات فارنزیک یا رفع مشکلات و تهدیدهای اعلام شده از سوی *امن‌پرداز* ایجاد شده است.
۲. اتفاقاتی که خارج از حیطه اختیار معقول *امن‌پرداز* می‌باشد، از قبیل موارد فورس ماجور: جنگ (سایبری یا غیر آن)، اعتصاب، قیام، حوادث طبیعی
۳. اتفاقاتی که در اثر عدم رعایت نکات ایمنی و امن‌سازی معقول سمت *بهره‌بردار* رخ دهند، از جمله و نه محدود به عدم توجه به پیاده‌سازی استانداردها، رمزنگاری‌ها، ویا اعمال سیاست‌های امنیتی، یا استفاده از کلمات عبور ضعیف، پیاده نکردن سیاست‌های حداقل دسترسی، عدم وجود بکاپ‌گیری منظم و صحیح و ...
۴. اتفاقاتی که در پنجره تعمیر و نگهداری برنامه‌ریزی شده خدمات رخ دهند.

بهره‌بردار تایید می‌کند که *امن‌پرداز* فناوری‌ها و فرایندهای تجاری منطقی را اجرا نموده و *امن‌پرداز* هیچگونه تضمینی ارائه نمی‌دهد که این خدمات قادر به شناسایی، پیشگیری یا کاهش اثرات صد در صد تمامی انواع حملات یا حوادث سایبری باشند.