

توافق نامه سطح خدمات

Padvish MXDR

شرکت نرم افزاری امن پرداز

سطح محرمانگی: عادی



شرکت نرم افزاری
امن پرداز

نسخه ۱.۰۰

بهار ۱۴۰۴

فهرست مطالب

۱. مقدمه	۳
۲. تعاریف و اصطلاحات	۴
۲.۱.۱. سطح خدمات	۶
۲.۲. مولفه های Padvish MXDR	۶
۲.۳. سطوح حساسیت هشدارهای امنیتی	۷
۳. محدوده خدمات	۸
۳.۱. مرحله راه اندازی	۸
۳.۲. بررسی دوره ای سلامت سیستم	۸
۳.۳. کشف، بررسی و پاسخ به رخداد	۹
۳.۴. زمان واکنش	۱۰
۳.۵. دسترس پذیری	۱۱
۳.۶. شکار تهدیدات	۱۱
۳.۷. گزارش دهی دوره ای	۱۱
۴. اعلام ادعا و دریافت اعتبار	۱۲
۴.۱. روش محاسبه اعتبار خدمات	۱۲
۴.۲. فرایند اعلام ادعا	۱۲
۵. تعهدات بهره بردار	۱۳
۶. استثنائات	۱۴

۱. مقدمه

این سند توافق نامه سطح خدمات مرکز کشف نفوذ و مقابله با تهدیدات پیشرفته Padvish MXDR را بیان می کند که شامل تعهدات خدمات و شرایط آن می باشد. در سرتاسر این سند، از لفظ «امن پرداز» به عنوان ارائه دهنده خدمات Padvish MXDR و از لفظ «بهره بردار» به عنوان کارفرما/مشری/استفاده کننده از خدمات فوق استفاده شده است.

مطالب این سند بخش اصلی اسناد قانونی فی مابین بهره بردار و امن پرداز را تشکیل می دهد و مکمل و جایگزین هر نوع تعهد مربوط به سطح خدمات Padvish MXDR می باشد که در سایر اسناد مکتوب یا غیرمکتوب فی مابین 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.

بهره بردار می پذیرد و موافقت می کند که امن پرداز ممکن است هر از چندگاهی بدون کاهش یا تضعیف عملکرد کلی خدمات خود، تغییراتی در آن بدهد و نیز امن پرداز می تواند محتویات این سند را جهت تطبیق با واقعیت خدمات ارائه شده اصلاح یا بروزرسانی نماید.

۲. تعاریف و اصطلاحات

رج	اصطلاح	شرح
۱.	امن پرداز	شرکت نرم افزار امن پرداز که ارائه دهنده خدمات Padvish MXDR می باشد
۲.	بهره بردار	مشتری/کارفرما یا هر شخصی که خدمات Padvish MXDR را خریداری کرده و لایسنس مربوطه را دریافت و قصد دارد در شبکه خود استفاده نماید
۳.	رابط بهره بردار	فرد یا افرادی که از سمت بهره بردار به امن پرداز جهت انجام هماهنگی های لازم معرفی می شود. این فرد/افراد باید دانش فنی و اختیارات لازم جهت فهم هشدارها و در دسترس قرار دادن فوری سیستم ها 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 MXDR خدمات مرکز کشف نفوذ و مقابله با تهدیدات پیشرفته Padvish MXDR می باشد.
۵.	طول دوره خدمات	حداصل بین تاریخ شروع خدمات تا پایان آن که توسط بهره بردار خریداری شده است.
۶.	هشدار	نفوذ تایید شده یا احتمال نفوذ به سیستم ها که تهدیدی برای امنیت دارایی های بهره بردار محسوب می شود.
۷.	سطح (حساسیت) هشدار	سطح هشدار یا سطح حساسیت هشدار، نشان دهنده میزان فوریت و نحوه برخورد با آن می باشد 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 بهره بردار و سپس اخذ دسترسی آغاز می شود. (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 ایجت گرفته تا نصب

وصله های امنیتی سیستم عامل و نرم افزارها و مانند آن. (اطلاعات بیشتر در بند ۳.۲)		
مقصود از تیم پاسخ به رخداد در این سند، تیمی از امن پرداز است که وظیفه نظارت، بررسی و پاسخ به رخدادهای امنیتی را دارد.	تیم پاسخ به رخداد	۱۱.
اعلام درخواست از سمت بهره بردار که تعهدات مندرج در این توافق نامه نقض شده و تقاضای اعتبار خدمات مطابق بند ۴	ادعا	۱۲.
مجوز نصب و استفاده از خدمات Padvish MXDR که از سمت امن پرداز برای استفاده در شبکه بهره بردار صادر شده و دارای ویژگی های مشخص مانند تاریخ شروع و پایان، تعداد ایجنت، و... می باشد.	لایسنس	۱۳.
مقصود از کلمه ایجنت یا ایجنت پادویش در این سند، نسخه ای از آنتی ویروس پادویش است که با لایسنس مرتبط با MXDR و تحت مدیریت مرکزی فعال شده باشد.	ایجنت (پادویش)	۱۴.
که به نام Padvish Management Server یا PMS نیز خوانده می شود، یک سرویس مرکزی مستقر در شبکه بهره بردار می باشد که مدیریت ایجنت های آنتی ویروس پادویش از طریق آن انجام می شود.	سرور مدیریت مرکزی پادویش	۱۵.
مولفه های محصول Padvish XDR که شامل انواع ماژول های سنسورها، داشبوردها، شکار تهدیدات، و ... می شود. (مطابق مستندات آن)	مولفه های Padvish XDR	۱۶.
سرور مرکزی سامانه MXDR که در محل امن پرداز وجود دارد و وظیفه جمع آوری، پردازش و کنترل این خدمات را برعهده دارد.	سامانه مرکزی Padvish MDR/MXDR	۱۷.
مجموعه دستگاه هایی که بهره بردار قصد حفاظت از آنها توسط خدمات Padvish MXDR را دارد، ایجنت پادویش روی آنها نصب بوده و با لایسنس مرتبط فعال و متصل به سامانه های مدیریتی و MXDR هستند.	دستگاه های تحت محافظت	۱۸.

۲/۱/۱. سطح خدمات

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

۲/۲. مولفه‌های Padvish MXDR

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

۱. ایجننت پادویش: نسخه‌ای به‌روز از آنتی‌ویروس پادویش که بر روی دستگاه‌های تحت محافظت، با لایسنس Padvish MXDR 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 ایجننت ممکن است منوط به ریست سیستم پس از نصب یا آپگرید آن باشد)
۲. سرور مدیریتی پادویش: نسخه‌ای به‌روز از سرور مدیریتی پادویش که بر روی یک یا چند سرور به صورت مستر/اسلیو درون شبکه بهره‌بردار نصب می‌شود و هر سرور، وظیفه مدیریت ایجننت‌های پادویش در محدوده خود را داراست. تمامی سرورهای مدیریتی پادویش - علاوه بر نیازمندی‌های

ارتباطی معمول خود که در سند نیازمندی های نصب به آن اشاره شده - باید با سامانه مرکزی Padvish MXDR اتصال بدون محدودیت داشته باشند.

۳. مجموعه سرورهای XDR پادویش: نسخه ای به روز از مجموعه کامل مولفه های Padvish XDR

که درون شبکه بهره بردار نصب بوده و ایجننت های پادویش و سرور(های) مدیریتی پادویش اطلاعات خود را به آنها ارسال می کنند. این سرورها نیز - علاوه بر نیازمندی های ارتباطی معمول خود که در سند نیازمندی های نصب محصول Padvish XDR به آن اشاره شده - باید اتصال بدون محدودیت با سامانه مرکزی Padvish MXDR داشته باشند.

۲/۳. سطوح حساسیت هشدارهای امنیتی

در مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MXDR) هشدارهای امنیتی از نظر درجه خطر و اهمیت به سطوح مختلفی تقسیم بندی می شوند که با رنگ هشدار مشخص می شود:

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

۲. هشدار قرمز (تماس فوری): احتمال جدی هک و نفوذ که باید فوراً 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 می باشد.

۳. محدوده خدمات

۳/۱. مرحله راه اندازی

در مرحله راه اندازی خدمات، بهره بردار باید عملیات زیر را انجام دهد:

۱. معرفی رابط: فرد یا تیم رابط بهره بردار 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 بهره بردار باید به صورت ۲۴x۷ جهت دریافت تماس های اضطراری در دسترس بوده و احاطه فنی مناسب و اختیارات لازم جهت فراهم کردن شرایط بررسی فوری دستگاه های در خطر را داشته باشد.
۲. نصب و فعالسازی کلیه مولفه های Padvish MXDR: بهره بردار باید کلیه مولفه های Padvish MXDR که در بخش ۲.۲ 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 MXDR: بهره بردار باید چنانکه در بخش ۲.۲ بیان شد، ارتباط مستقیم سرور(های) مدیریتی پادویش و مولفه های Padvish XDR را با سامانه مرکزی Padvish MXDR برقرار نموده و تست نماید.

۳/۲. بررسی دوره ای سلامت سیستم

۱. سلامت سیستم، شامل مجموعه ای از عوامل به شرح زیر است:
 - a. وجود پیکربندی صحیح،
 - b. فعال بودن کامل محافظت ها،
 - c. متصل بودن ایجنت ها به سرورهای مدیریتی پادویش
 - d. متصل بودن ایجنت ها به سرورهای Padvish XDR،
 - e. متصل بودن تجهیزات زیرساختی (مجازی سازی، ذخیره سازی، بکاپ گیری، شبکه) به سرورهای Padvish XDR،
 - f. دریافت کامل ترافیک خام شبکه از کلیه vlan های مورد نظارت و متصل بودن سنسور ترافیک شبکه به سرورهای Padvish XDR،
 - g. متصل بودن سرورهای مدیریتی پادویش به سامانه مرکزی Padvish MXDR

- h. متصل بودن سرورهای Padvish XDR به سامانه مرکزی Padvish MXDR.
 - i. به روز بودن سیستم عامل و نرم افزارهای شخص ثالث،
 - j. صحت و سینک بودن تاریخ سیستم
 - k. به روز بودن پایگاه امضا، و نیز نسخه ایجنت و سایر مولفه های Padvish MXDR.
 - l. عدم وجود اکانت ها با پسوردهای ضعیف، قابل حدس، یا مشابه،
 - m. وجود پشتیبان به روز و کامل از داده ها،
 - n. عدم وجود هشدار امنیتی بر روی سیستم ها
 - o. و به طور کلی رعایت نکات امنیتی استاندارد و معقول
۲. بهره بردار باید به صورت دوره های حداقل هفتگی، وضعیت سلامت سیستم ها را بررسی نموده و اقدامات لازم مانند آپدیت کردن، بکاپ گرفتن، اعمال کردن سیاست های امنیتی و... را جهت رفع نواقص انجام دهد. در صورتیکه اقدامات لازم جهت رفع موضوع توسط بهره بردار انجام نگیرد، کاهش توانایی خدمات در تشخیص تهدیدات امنیتی که در اثر این موضوع ایجاد شود به عهده بهره بردار خواهد بود.
۳. تیم پاسخ به رخداد امن پرداز زیر از سلامت سیستم را بررسی نموده و در صورت نقض موارد امنیتی به صورت هشدار اعلام می کند. وظیفه رفع موارد اعلامی با بهره بردار خواهد بود:
- a. متصل بودن سرورهای مدیریتی پادویش به سامانه مرکزی Padvish MXDR
 - b. متصل بودن سرورهای Padvish XDR به سامانه مرکزی Padvish MXDR.
 - c. خاموش شدن کامل یک محافظت: این مورد فقط ناظر به تغییرات جدید بوده و تنظیماتی که قبل یا حین مرحله راه اندازی انجام شده باشد را شامل نمی شود. این مورد شامل خاموش بودن بخشی از یک محافظت یا پیکربندی اشتباه آن نمی شود.

۳/۳. کشف، بررسی و پاسخ به رخداد

تیم پاسخ به رخداد امن پرداز زیر را برای کشف، بررسی و پاسخ به رخداد های امنیتی انجام می دهد:

۱. پردازش: اطلاعات تشخیص ها و سنسورها پردازش می شوند تا موارد مهم و نشانه های 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 راه اندازی با رابط بهره بردار تماس گرفته و هشدار را اعلام می نماید. پس از اعلام، وظیفه دادن دسترسی به سیستم (ها) جهت عملیات فارنزیک توسط تیم پاسخ به رخداد امن پرداز با رابط بهره بردار خواهد بود.

۳. عملیات فارنزیک: عملیات فارنزیک برای اطمینان از صحت هشدارها انجام می گیرد، 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 می شود. 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: بهره بردار می پذیرد که موافقت وی برای بررسی سیستمها توسط امن پرداز 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 بهره بردار می پذیرد که عدم موافقت برای بررسی سیستمها یا ایجاد تغییرات می تواند منجر به فعالیت مخرب جدید یا بدتر شدن وضعیت امنیتی گردد. اگر بهره بردار درخواست امن پرداز را برای بررسی یا انجام تغییرات رد نموده یا در آن تاخیر ایجاد نماید، امن پرداز هیچ تعهدی برای هیچگونه خسارتی که در اثر عملیات مخرب ایجاد می شود 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 بهره بردار (از طریق ایمیل، پیامک، یا تلفن) پایان می یابد.

حداکثر زمان واکنش در مورد انواع سطوح حساسیت هشدار به شرح جدول زیر می باشد:

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)

امن پرداز متعهد می شود که در خصوص هشدارهای با سطح حساسیت فوری (قرمز/سیاه)، زمان واکنش حداکثر ۳۰ دقیقه باشد. در صورتیکه امن پرداز موفق نشود این تعهد را برآورده کند، بهره بردار می تواند مطابق بند ۴ وارد فرایند اعلام/دعا و دریافت اعتبار گردد.

۳/۵. دسترس پذیری

تمامی عملیات کشف، بررسی و پاسخ به رخداد (بند ۳.۳) توسط تیم پاسخ به رخداد امن پرداز به صورت ۲۴×۷×۳۶۵ انجام می گیرند. به علاوه بهره بردار می تواند 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 امن پرداز به صورت فعال نشانه های تهدیداتی که از کنترل های تشخیص موجود گذشته باشند را جستجو می کند. این جستجو در اطلاعاتی انجام می شود که توسط سنسورها از روی دستگاه های تحت محافظت جمع آوری شده اند و بر اساس تشخیص رفتارها یا تاکتیک های مشابهی که قبلا توسط نفوذگران استفاده شده اند یا روش های ابداعی جدید انجام می گیرد. در صورت کشف رفتار مشکوک، با توجه به سطح حساسیت هشدار، فرایند پاسخ به رخداد (بند ۳.۳) انجام خواهد گرفت.

۳/۷. گزارش دهی دوره ای

امن پرداز به صورت دوره ای ماهانه یا فصلی، گزارشی از تشخیص ها، هشدارها، اقدامات انجام شده در پاسخ به رویداد، و توصیه های امنیتی جهت بهبود وضعیت امنیت شبکه به رابط بهره بردار ارسال می نماید.

۴. اعلام ادعا و دریافت اعتبار

۴/۱. روش محاسبه اعتبار خدمات

در صورتیکه امن پرداز نتواند به تعهد خود در خصوص زمان واکنش در هشدارهای با سطح حساسیت فوری عمل نماید، بهره بردار 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. بهره بردار در هر روز تقویمی می تواند حداکثر یک ادعا ثبت نماید.

۴/۲. فرایند اعلام ادعا

۱. به منظور واجد شرایط بودن برای ارائه ادعا و دریافت اعتبار، بهره بردار باید ابتدا با استفاده از رویه های تعیین شده توسط امن پرداز، ظرف حداکثر ۱۴ روز تقویمی پس از تاریخ اعلام هشدار، پشتیبانی امن پرداز را از رخداد آن مطلع کند.

۲. برای ارسال یک ادعا، بهره بردار 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 بهره بردار بیش از ۱۴ روز گردد، امکان ثبت و دریافت ادعا منقضی شده تلقی خواهد شد.

۴. امن پرداز 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 بهره بردار افزوده خواهد شد.

۵. تعهدات بهره بردار

بهره بردار متعهد می شود که وظایف زیر را انجام دهد:

۱. مشخص نمودن یک رابط بهره بردار که با تیم پاسخ به رخداد امن پرداز همکاری نماید. بهره بردار اطمینان حاصل می کند که اطلاعات رابط بهره بردار و اطلاعات تماس نزد امن پرداز به روز و صحیح باشد.
۲. رابط بهره بردار باید از دانش فنی و اختیارات لازم جهت دادن دسترسی کامل، به موقع و سریع به تیم پاسخ به رخداد امن پرداز جهت بررسی سیستم ها و تجهیزات (روی دستگاه های تحت محافظت یا غیر آن) در زمان مواجهه با هشدارهای امنیتی برخوردار باشد. به علاوه باید دانش فنی و اختیارات لازم جهت اعمال توصیه های امنیتی و پاکسازی تهدیدات و امن سازی پیکربندی های اعلام شده را داشته باشد.
۳. حصول اطمینان از صحت ارتباطات لازم چنانکه در بخش ۲.۲ گذشت.
۴. حصول اطمینان از صحت نصب و فعال سازی، صحت پیکربندی، صحت عملکرد، به روز بودن و متصل بودن ایجنت های پادویش، سیستم عامل و نرم افزارها و در یک کلمه بررسی دوره ای سلامت سیستم (بند ۳.۲) بر روی دستگاه های تحت محافظت
۵. انجام کامل عملیات مرحله راه اندازی مطابق بند ۳.۱
۶. حصول اطمینان از عدم وجود فناوری ها یا پیکربندی هایی که با مسدود کردن ترافیک، حذف لاگ ها، 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 توصیه های امنیتی ارائه شده به بهره بردار توسط امن پرداز و یا اشخاص ثالث در سریعترین زمان ممکن
۹. تهدیداتی که از سمت دستگاه ها و تجهیزاتی که جزو دستگاه های تحت محافظت نیستند (به عنوان مثال همه دستگاه هایی که نسخه به روز و فعال شده با لایسنس مناسب MXDR از ایجنت بر روی آنها نصب نیست) ایجاد می شوند خارج از حیطه این خدمات و توافق نامه می باشند و مسئولیت آنها با بهره بردار می باشد.

۱۰. عملیات و اقداماتی که به صراحت در این توافق نامه قید نشده اند جزئی از خدمات نمی باشند و مسئولیت آنها با بهره بردار می باشد. به علاوه بهره بردار می پذیرد که امن پرداز مسئول تهدیداتی که پیش از تاریخ آغاز خدمات در شبکه وجود داشته اند نمی باشد.

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

۶. استثنائات

بهره بردار می پذیرد که امن پرداز مسئولیتی در قبال اتفاقات زیر ندارد:

۱. اتفاقاتی که به دلیل تاخیر توسط بهره بردار در دادن دسترسی جهت عملیات فارتزیک یا رفع مشکلات و تهدیدهای اعلام شده از سوی امن پرداز ایجاد شده است.

۲. اتفاقاتی که خارج از حیطه اختیار معقول امن پرداز می باشد، از قبیل موارد فورس ماجور: جنگ (سایبری یا غیر آن)، اعتصاب، قیام، حوادث طبیعی

۳. اتفاقاتی که در اثر عدم رعایت نکات ایمنی و امن سازی معقول سمت بهره بردار رخ دهند، از جمله و نه محدود به عدم توجه به پیاده سازی استانداردها، رمزنگاری ها، ویا اعمال سیاست های امنیتی، یا استفاده از کلمات عبور ضعیف، پیاده نکردن سیاست های حداقل دسترسی، عدم وجود بکاپ گیری منظم و صحیح و ...

۴. اتفاقاتی که در پنجره تعمیر و نگهداری برنامه ریزی شده خدمات رخ دهند.

بهره بردار تایید می کند که امن پرداز فناوری ها و فرایندهای تجاری منطقی را اجرا نموده و امن پرداز هیچگونه تضمینی ارائه نمی دهد که این خدمات قادر به شناسایی، پیشگیری یا کاهش اثرات صد در صد تمامی انواع حملات یا حوادث سایبری باشند.

شرکت نرم افزار امن پرداز[®]

Amnpardaz Software Corporation[®]



w w w . a m n p a r d a z . c o m