شرکت فناوری سپهر امن پارسین

نام سند	طرح تداوم و بازیابی سرویس		
شماره سند		تعداد صفحات	۱۹

فرایند تصویب		
تهیه‌کننده	تأییدکننده	تصویب‌کننده
		مدیرعامل
تاریخ و امضاء:	تاریخ و امضاء:	تاریخ و امضاء:

شکل مجاز قابل استفاده

☒ چاپ شده (کاغذی)
☒ بر روی سایت اینترانت شرکت فناوری سپهر امن پارسین (الکترونیکی)
☐ بر روی سایت اینترنتی شرکت فناوری سپهر امن پارسین (الکترونیکی)
☒ پوشه اشتراکی

طبقه‌بندی: ☐ دسترسی عادی (فاقد طبقه‌بندی)/ ☐ سازمانی/ ☒ محرمانه

دسترسی مجاز:
☒ کلیه واحدهای مرتبط
☐ برون‌سازمانی
☐ واحدهای خاص

توجه: «از چاپ، کپی و توزیع این مستند بدون داشتن مجوز کتبی اکیداً خودداری کنید».

شرح بازنگری

شماره بازنگری	تاریخ بازنگری	شرح و علت تغییرات (تغییر، تدوین و منسوخ شدن سند)	صفحه بازنگری	تصویب‌کننده

روند کنترل سند

مسئول کنترل:	سمت:	تاریخ:	
مستند به لحاظ رعایت مسائل املایی و نگارشی مورد تأیید است؟			☑
مستند به لحاظ رعایت شکل استاندارد مورد تأیید است؟			☑
مستند به لحاظ محتوایی و رعایت اصول فنی و تخصصی مورد تأیید است؟			☑
مدارک مرتبط و مدارک زیرمجموعه مستند در محل مناسب قید شده و به درستی طراحی، تدوین و شماره‌دهی شده‌اند؟			☑
روال تهیه، تأیید و تصویب مدرک بر اساس روند روش اجرایی کنترل اطلاعات مستند انجام شده است؟			☑
فایل الکترونیکی جهت استفاده کاربران مجاز به صورت PDF درآمده و قابل دسترس است؟			☑

فهرست مطالب

۱ مقدمه

طرح تداوم کسب‌وکار (BCP[۱]) در یک نگاه کلی مجموعه‌ای از روش‌ها و دستورالعمل‌های فنی و فرایندی است که به صورت ساختارمند به حوزه تداوم کسب‌وکار پرداخته و به دنبال آن است که از بروز بحران و ایجاد وقفه برای هر یک از سرویس‌های حیاتی شرکت جلوگیری کند. طرح بازیابی از فاجعه (DRP[۲]) نیز بخشی از سند BCP است که نگاه ویژه‌ای به مرحله گذار از بحران داشته و در پی آن است در صورت بروز یک حادثه یا رخداد، اقدام‌های لازم برای گذار از آن بحران در کوتاه‌ترین زمان ممکن به عمل آید.

در این مستند به فرایند استمرار مدیریت و تداوم کسب‌وکار و بازیابی از فاجعه سرویس ..... پرداخته می‌شود. همچنین به زیرساخت‌های مورد نیاز جهت ایجاد استمرار خدمات‌دهی این سرویس نیز اشاره خواهد شد.

۲ اطلاعات سامانه/ سرویس

آخرین نسخه سامانه/ سرویس			
Version	**Release**	**تاریخ**	**محل نگهداری**

نام سرور و IP Addressهای سامانه/ سرویس

نام سرور برنامه					
نام و آدرس سرور پایگاه داده					
شبکه محلی	**شبکه دولت**	**شبکه ملی**	**MPLS تهران**	**MPLS استانی**	**سایر**

منابع مورد نیاز برای راه‌اندازی سامانه/ سرویس

پارامتر	توضیحات
نوع و ورژن سیستم‌عامل سرور سامانه	
نوع و ورژن سیستم‌عامل سرور پایگاه داده	
نوع و ورژن پایگاه داده	

[۱] Business Continuity Plan

[۲] Disaster Recovery Plan

کلمات عبور	
سایر منابع یا نرم‌افزارهای مورد نیاز	

حداقل منابع برای راه‌اندازی سرور برنامه			
RAM	CPU	HDD	Other

حداقل منابع برای راه‌اندازی سرور پایگاه داده سامانه			
RAM	CPU	HDD	Other

۳ اسناد حیاتی سامانه/ سرویس

راهنمای نصب و راه‌اندازی سامانه/ سرویس				
محل نگهداری فایل فیزیکی	محل نگهداری فایل الکترونیکی	نام فایل الکترونیکی	مسئول	شماره تماس

تذکر: یک نسخه از فایل، به صورت الکترونیکی یا فیزیکی پیوست سند گردد.

راهنمای بهره‌برداری از سامانه/ سرویس				
محل نگهداری فایل فیزیکی	محل نگهداری فایل الکترونیکی	نام فایل الکترونیکی	مسئول	شماره تماس

تذکر: یک نسخه از فایل، به صورت الکترونیکی یا فیزیکی پیوست سند گردد.

٤ وضعیت سامانه/ سرویس

در لایه مجازی‌سازی، زیرساخت پیاده‌سازی شده برای این سامانه/ سرویس به صورت شکل شماره ۱ است:

معماری سامانه/ سرویس

شکل ۱: وضعیت فعلی سامانه/ سرویس

این سامانه/ سرویس با ذینفعان زیر در ارتباط است:

- .....
- .....
- .....

تحلیل جریان کاری اصلی سامانه/ سرویس

کلیه اطلاعات و سامانه‌های فعال سرویس که به طور مستقیم در ارائه خدمت به بهره‌برداران مورد استفاده قرار می‌گیرند، به صورت شکل شماره ۲ در محیط عملیاتی مستقر هستند:

معماری لایه عملیاتی سرویس

شکل ۲: وضعیت معماری لایه عملیاتی سرویس

درخواست کاربران از طریق مسیر زیر هدایت گردیده و اختلال در عملکرد هر کدام از آنها منجر به ایجاد اشکال مستقیم در عملکرد سرویس خواهد شد:

نمونه

- لایه کاربر: شخصی که کاربر سرویس است.
- لایه اپلیکیشن: که خود شامل دو دسته زیر می‌باشد:
  - کسب‌وکاری: مرتبط با بخش‌های تولیدی شرکت
  - فنی: مرتبط با واحدهای مربوطه در شرکت
- لایه پایگاه داده: در ارتباط با واحد دیتابیس شرکت
- لایه زیرساخت و شبکه: مشتمل بر سرورها (اعم از فیزیکی یا مجازی)، محیط ذخیره‌سازی، ارتباطات شبکه‌ای و سرویس‌های شبکه.

تحلیل جریان کاری پشتیبان سامانه/ سرویس

علاوه بر سرورهای کلیدی، از سرورهای پشتیبان نیز استفاده می‌شود که مسئولیت حفظ کیفیت خدمات‌دهی سامانه/ سرویس را بر عهده داشته و به طور مستقیم در درخواست کاربران و ارایه سرویس نقشی ندارند. معماری و لیست این سرورها در لایه عملیاتی به شرح زیر است:

معماری سرورهای پشتیبان

شکل ۳: وضعیت معماری سرورهای پشتیبان سرویس

- سرور ..... : ..... توضیحات
- سرور ..... : ..... توضیحات
- سرور ..... : ..... توضیحات

مثال ۱: سرور PRTG: یک نرم‌افزار نظارت بر شبکه است. نرم‌افزار PRTG می‌تواند شرایطی مانند میزان استفاده از پهنای باند یا UPTIME سرویس‌ها و همچنین منابع سخت‌افزاری سرورها را پایش و طبقه‌بندی کرده و آمار را بر اساس هاست‌های مختلف جمع‌آوری نماید.

مثال ۲: سرور NTP: یک ماشین مجازی است که زمان دقیق را از سرورهای جهانی دریافت کرده و وظیفه هماهنگ‌سازی زمانی را بین نودهای موجود در یک شبکه بر عهده دارد.

مثال ۳: AVBoard: سامانه داشبورد مدیریتی سامانه که اطلاعات لازم را برای راهبری لایه کسب‌وکار سامانه در اختیار راهبران آن قرار می‌دهد.

تحلیل وضعیت مرکز داده

کلیه ماشین‌های در اختیار این سرویس، در مرکز داده شرکت مستقر بوده و ..... سرور فیزیکی از نوع ..... HP به آن اختصاص یافته است. لازم به ذکر است رعایت اصل اجتناب از Single Point of Failure در حوزه مرکز داده بسیار مهم می‌باشد. لذا از جمله اقدام‌های صورت گرفته در این خصوص می‌توان به موارد زیر اشاره کرد:

- وجود vSphere Cluster برای افزونگی حوزه پردازشی
- استفاده از SAN Storage برای ذخیره‌سازی کلیه داده‌ها و اطلاعات
- استفاده از افزونگی لازم در شبکه‌های Ethernet و FiberChannel
- استفاده از تجهیزات مناسب امنیت شبکه (مانند Firewall, IDPS, SIEM)
- در نظر گرفتن قطعات یدکی اضافی جهت جایگزینی سریع قطعات معیوب حیاتی
- وجود افزونگی لازم در زیرساخت‌های فیزیکی (مانند Cooling و UPS)
- وجود زیرساخت‌های کمکی (مانند Diesel Generator و Fire Detection System)
- وجود استحکامات لازم برای مقابله با بلایای طبیعی همچون سیل و زلزله
- وجود تیم فنی مناسب و فرایندهای مشخص و مدون برای مقابله با اشکالات و تهدیدها.

۵ ارزیابی و تحلیل مخاطرات مربوط به تداوم فعالیت سرویس

بررسی مخاطرات وضعیت موجود بسیار حائز اهمیت بوده و مشخص‌کننده عوامل اصلی ایجاد اختلال در استمرار سرویس می‌باشد. در ابتدا به انواع دارایی‌ها و عوامل تهدید اشاره کرده و سپس در بندهای بعدی، به درجات ریسک و نحوه ارزیابی و مدیریت آنها پرداخته

می‌شود.

دارایی‌ها

در این بخش به بررسی دارایی‌های مرتبط با سرویس پرداخته می‌شود. این دارایی‌ها شامل دسته‌بندی‌های زیر هستند:

- داده‌ها و اطلاعات سامانه/ سرویس
- نرم‌افزارها، برنامه‌های کاربردی و سامانه‌های عملیاتی
- زیرساخت پردازشی و ذخیره‌سازی مرکز داده
- راهبران و کاربران
- تجهیزات شبکه و امنیت

عوامل تهدید

در این بخش به بررسی عوامل تهدید مرتبط با سرویس پرداخته می‌شود. انواع عوامل تهدید به شرح زیر است:

- انواع خرابی در تجهیزات فیزیکی
- عوامل طبیعی
- اشتباه‌ها و خطاهای انسانی
- هکرها و نفوذگران سایبری
- استفاده نادرست از سرویس توسط کاربران نهایی
- تأمین‌کنندگان سرویس‌های بیرونی
- پیمانکار سرویس.

٦ انواع و طبقه‌بندی مخاطرات

طبقه‌بندی و ارزش‌گذاری مخاطرات، یک بخش مهم در شناخت و اولویت‌بندی آنها محسوب می‌شود. در جدول زیر، تعریف انواع سطوح و معیارهای ارزش‌گذاری مخاطرات ارایه شده است.

سطوح و معیارهای میزان خرابی

معیار	ارزش کمی	توضیح
کم	**۱**	**در صورت بروز تهدید، همزمانی آن با سایر اتفاق‌ها و رویدادها می‌تواند منجر به ایجاد پیامدی در سطح متوسط شود.**
متوسط	**۲**	**در صورت بروز تهدید، امکان قطع دسترسی موقت به سرویس وجود دارد.**
زیاد	**۳**	**در صورت بروز تهدید، امکان از دست رفتن اطلاعات یا احتمال قطع دسترسی به سرویس**

		به صورت طولانی‌مدت وجود دارد.

سطوح و معیارهای ارزش‌گذاری احتمال وقوع تهدید

معیار	ارزش کمی	توضیح
کم	۱	احتمال وقوع تهدید برای دارایی پایین است.
متوسط	۲	احتمال وقوع تهدید برای دارایی متوسط است.
زیاد	۳	احتمال وقوع تهدید برای دارایی بالا است.

۷ تحلیل مخاطرات

در این بخش، به شناسایی مخاطرات و ارایه راهکار مناسب برای هر یک از آنها پرداخته می‌شود. این مخاطرات در سه حوزه «زیرساخت و سخت‌افزار»، «نرم‌افزار و سامانه» و «کسب‌وکار»، شناسایی و ارزش‌گذاری شده و در بخش ارزیابی مخاطرات سرویس، مورد بهره‌برداری قرار گرفته‌اند. فرمول نهایی ارزش ریسک، حاصل جمع مقادیر احتمال وقوع و میزان خرابی، بر اساس جداول فوق می‌باشد.

لازم به ذکر است به منظور ارزیابی و مدیریت مخاطرات سرویس، همچنین می‌توان از رویه ارایه شده در روش اجرایی مدیریت مخاطرات شرکت نیز استفاده کرد.

نمونه

#	حوزه	ریسک	احتمال وقوع	میزان خرابی	ارزش ریسک
۱	نرم‌افزار و سامانه	قطعی یا اختلال در سرویس‌دهی به دلیل بستر سیستم‌عاملی نامناسب	کم	متوسط	۴
۲	نرم‌افزار و سامانه زیرساخت و سخت‌افزار	نفوذ به سامانه/ سرویس یا شبکه به دلیل ثبت ناموفق رویدادها و رخدادهای امنیتی و همچنین پایش آنها	کم	متوسط	۴
۳	نرم‌افزار و سامانه	دسترسی غیرمجاز به سامانه/ سرویس به دلیل دریافت اطلاعات خاص ناشی از عدم پیکربندی صحیح آن	کم	زیاد	۶
۴	نرم‌افزار و سامانه	دسترسی غیرمجاز به سامانه/ سرویس به دلیل پیکربندی نامناسب کنترل دسترسی و ضعف در رعایت حقوق دسترسی	کم	زیاد	۶
۵	نرم‌افزار و سامانه	شنود اطلاعات به دلیل عدم وجود سیاست رمزنگاری نام کاربری و کلمه عبور	کم	زیاد	۶
۶	نرم‌افزار و سامانه	شنود اطلاعات به دلیل استفاده از رمزنگاری ضعیف در تبادل داده‌ها	کم	زیاد	۶
۷	نرم‌افزار و سامانه	نشت اطلاعات به دلیل عدم وجود سیاست غیرفعال نمودن نام کاربری پس از چندین‌بار تلاش ناموفق	کم	زیاد	۶

۸	نرم‌افزار و سامانه زیرساخت و سخت‌افزار	قطعی یا اختلال در سرویس‌دهی به دلیل ارتقا یا به‌روزرسانی سامانه/ سرویس	متوسط	متوسط	۵
۹	نرم‌افزار و سامانه زیرساخت و سخت‌افزار	اختلال در سرویس‌دهی به دلیل عدم ارتقا یا به‌روزرسانی سامانه/ سرویس	متوسط	متوسط	۵
۱۰	نرم‌افزار و سامانه زیرساخت و سخت‌افزار	قطعی یا اختلال در سرویس‌دهی به دلیل عدم وجود افزونگی کافی	زیاد	زیاد	۸
۱۱	نرم‌افزار و سامانه زیرساخت و سخت‌افزار	قطعی یا اختلال در سرویس‌دهی به دلیل آلودگی بدافزاری	کم	متوسط	۴
۱۲	کسب‌وکار	وقفه و اختلال در سرویس‌دهی به دلیل دسترسی غیرمجاز به سامانه/ سرویس و سرویس‌های مرتبط با آن	کم	زیاد	۶
۱۳	کسب‌وکار	نفوذ به سامانه/ سرویس به دلیل سیستم احراز هویت نامناسب	کم	زیاد	۶
۱۴	کسب‌وکار زیرساخت و سخت‌افزار نرم‌افزار و سامانه	اختلال در سرویس‌دهی به دلیل عدم پشتیبانی مناسب	کم	متوسط	۴
۱۵	زیرساخت و سخت‌افزار	قطعی یا اختلال در سرویس‌دهی به دلیل عدم وجود افزونگی خطوط ارتباطی شبکه	زیاد	متوسط	۶
۱۶	نرم‌افزار و سامانه زیرساخت و سخت‌افزار	نفوذ به سامانه/ سرویس و شبکه به دلیل عدم به‌روزرسانی و نصب وصله‌های امنیتی	متوسط	زیاد	۷
۱۷	زیرساخت و سخت‌افزار	قطعی یا اختلال در سرویس‌دهی به دلیل اشتباه در محاسبه ظرفیت منابع مورد نیاز	کم	متوسط	۴
۱۸	زیرساخت و سخت‌افزار	قطعی یا اختلال در سرویس‌دهی به دلیل ایجاد اشکالات سخت‌افزاری، قطعی یا نوسانات برق	متوسط	متوسط	۵
۱۹	زیرساخت و سخت‌افزار	خرابی تجهیزات و اختلال در سرویس‌دهی به دلیل نوسانات برق، دما و رطوبت	کم	متوسط	۴
۲۰	زیرساخت و سخت‌افزار	قطعی و اختلال در سرویس‌دهی به دلیل کارکرد نامناسب سیستم سرمایشی	کم	متوسط	۴

۲۱	کسب‌وکار زیرساخت و سخت‌افزار نرم‌افزار و سامانه	قطعی و اختلال در سرویس‌دهی به دلیل عدم مانیتورینگ مناسب	کم	متوسط	۴

۸ راهکارهای ارتقای تداوم سرویس

راهکارهای ارتقای دسترس‌پذیری سرویس، به دو بخش استمرار فعالیت سرویس (تداوم سرویس و پیشگیری از عدم خدمات‌دهی آن) و طرح عبور از بحران تقسیم می‌شود که در ادامه به بررسی آنها پرداخته می‌شود.

بهبود ساختار موجود

پس از شناخت وضعیت موجود، هدف‌گذاری RTO و RPO برای سرویس که مبتنی بر ساختار وضعیت فعلی باشد، بسیار حائز اهمیت است.

شاخص	زمان پیشنهادی	توضیحات
RTO	**.... ساعت**	**طراحی زیرساخت و سرویس باید به گونه‌ای باشد که در زمان بروز اشکال، سرویس در ..... ساعت مجدداً احیا و راه‌اندازی شود.**
RPO	**.... ساعت**	**طراحی طرح پشتیبان‌گیری باید به نحوی باشد که امکان احیای داده‌های سامانه/ سرویس تا ..... ساعت قبل امکان‌پذیر باشد.**
MAO	**.... ساعت**	**میزان زمان قطعی قابل قبول برای سامانه/ سرویس است.**
MBCO		**سطوح قابل قبول برای راه‌اندازی سرویس با کمترین منابع مورد نیاز به شرح زیر است:** **- وجود سرویس پشتیبان که در صورت قطعی و ایجاد خرابی در سرویس اصلی، امکان سوئیچ خودکار به آن وجود داشته باشد.** **- در نظر گرفتن منابع سخت‌افزاری لازم به صورت اسپیر و یدکی، جهت راه‌اندازی مجدد سرویس در کوتاه‌ترین زمان ممکن.**

برای نیل به اهداف زمانی بالا، موارد زیر پیشنهاد می‌شود (دیدگاه تداوم سرویس و رویکرد پیشگیرانه):

نمونه

ردیف	راهکار پیشنهادی	اهمیت	توضیحات
۱	ایجاد افزونگی در منابع پردازشی مرکز داده	بالا	لازم است افزونگی لازم در سطح سخت‌افزاری و منابع پردازشی اختصاصی سرویس در نظر گرفته شود.
۲	ایجاد افزونگی لازم در زیرساخت‌های مرکز داده	بالا	تمامی زیرساخت‌های کلیدی مرکز داده مرتبط با سرویس باید دارای افزونگی کافی باشند. راه‌اندازی قابلیت کلاسترینگ بسیار مهم است.
۳	ایجاد افزونگی لازم برای خطوط پشتیبان	بالا	خطوط ارتباطی اصلی باید دارای افزونگی کافی بوده و از طریق دو مسیر مجزا فراهم شوند.
۴	نگهداری داده‌های پشتیبان در مکان امن	بالا	لازم است یک نسخه پشتیبان به‌روز آفلاین، در محیط دیگری غیر از مرکز داده اصلی (سایت DR) به صورت امن نگهداری شود.

۹ طرح عبور از بحران

اتفاق‌های متعددی می‌تواند منجر به قطع کامل سرویس در مرکز داده اصلی شود. لذا استفاده از مرکز داده دوم در کنار فرایندهای مناسب می‌تواند تمهید مناسبی برای بازگشت سریع از بحران و وضعیت خرابی باشد. مرکز داده پشتیبان را می‌توان در سطوح مختلفی طراحی و پیاده‌سازی کرد. میزان RTO و RPO در زمان از دست رفتن مرکز داده اصلی، با به‌کارگیری هر سطح نیز متفاوت خواهد بود.

سطوح مرکز داده پشتیبان	توضیحات	RPO	RTO
بدون مرکز داده پشتیبان			
دارای مرکز داده پشتیبان			

از جمله تمهیداتی که در هنگام پیاده‌سازی مرکز داده پشتیبان باید به آنها توجه داشت می‌توان به موارد زیر اشاره کرد:

- پیاده‌سازی راهکار مناسب انتقال کاربران بین مراکز داده
- پیاده‌سازی لینک‌های ارتباطی بیرونی در مرکز داده دوم
- پیاده‌سازی لینک ارتباطی پایدار و باکیفیت بین دو مرکز داده.

➢ مرکز داده پشتیبان – Data Backup

پشتیبان‌گیری از داده‌ها و انتقال آنها به مکانی امن، اهمیت بسیار بالایی در تداوم سرویس دارد. از این رو، پیشنهاد پشتیبان‌گیری به شرح زیر است:

محتوای پشتیبان‌گیری	نوع	فاصله بین بکاپ	زمان نگهداری

لازم است کلیه اطلاعات فوق در مرکز داده دوم نیز نگهداری شده تا در زمان وقوع بحران بتوان به اطلاعات پشتیبان گرفته شده دسترسی داشت.

۱۰ افراد مؤثر در تداوم و بازیابی سرویس

افراد کلیدی و مؤثر در تداوم و بازیابی سرویس، به شرح جدول زیر هستند:

ردیف	نام شرکت/ واحد کسب‌وکاری	نام و نام خانوادگی	سمت	نقش/ وظیفه	شماره تماس	
					ثابت	همراه
۱						
۲						
۳						
۴						
۵						

۱۱ فرایند بازگردانی سرویس

❖ فاز فعال‌سازی (Activation)

پس از وقوع حادثه که می‌تواند با آگاهی یا عدم آگاهی از آن همراه باشد، فرایند بازگردانی و بازیابی سرویس آغاز می‌شود. در این فاز، سه مرحله اساسی وجود دارد که عبارتند از:

۱. اطلاع‌رسانی (Notification)

اقدام اطلاع‌رسانی یکی از مهمترین بخش‌های شروع فرایند بازگردانی سرویس‌ها است. بنابراین از طریق تلفن سازمانی و موبایل افراد (رجوع به جدول اطلاعات تماس) اطلاع‌رسانی به افراد مؤثر مرتبط با سرویس آغاز می‌شود. اطلاع‌رسانی می‌بایست شامل موارد ذیل باشد:

- توضیح اولیه در خصوص حادثه
- خرابی‌ها و مشکلات پیش آمده

- مکان یا زمان جلسه فوری
- تشریح وظایف فوری افراد.

۲. برآورد خسارت

پس از وقوع حادثه، اولین فرد/ تیم که آگاه شده و در محل حادثه حاضر می‌شود، کارشناس/ تیم برآورد خسارات است. وظیفه این بخش شامل موارد ذیل است:

- بررسی شواهد و موارد اطلاع داده شده
- بررسی امکان وقوع حوادث دیگر پس از حادثه اولیه
- بررسی بخش‌های دچار حادثه
- بررسی وضعیت فیزیکی
- بررسی وضعیت تجهیزات اصلی سرویس‌دهنده
- بررسی نوع حادثه از نگاه مهندسی
- بررسی تجهیزات و مواردی که می‌بایست تعویض شوند.
- بررسی زمان بازگشت به حالت اولیه سرویس، در صورتی که فرایند بازگردانی به حالت اولیه آغاز نشود (زمان فرایندهای نرمال نصب مجدد).

۳. برنامه‌ریزی بازگردانی

پس از اطمینان از وقوع حادثه و نیاز به فعال‌سازی طرح بازگردانی سرویس می‌بایست اقدام‌های لازم صورت پذیرد. مستند برنامه‌ریزی شامل بخش‌های ذیل است:

- لیست سیستم‌ها و سرویس‌هایی که می‌بایست بازگردانی شوند.
- فرایند و ترتیب بازگردانی و ارتباط بخش‌ها با یکدیگر
- میزان زمان تقریبی هر بازگردانی
- روش اعلام خرابی به مدیر هر بخش در صورت عدم موفقیت
- روش ارتباط بین بخش‌های درگیر در بازگردانی.

❖ فاز عملیات (Execution)

برنامه بازگردانی سرویس، پس از تهیه و ارایه برنامه بازگردانی و همچنین اطلاع‌رسانی به افراد و تیم‌های درگیر آغاز می‌شود. این فاز بر اساس مستند برنامه‌ریزی شکل می‌گیرد که پوشش‌دهنده موارد زیر است:

- دریافت دسترسی به سیستم‌های آسیب‌دیده یا مناطق خاص
- آگاه‌سازی کاربران ذینفع سیستم‌های آسیب‌دیده

- تعیین مکان مناسب جهت انجام کارهای تیمی
- دریافت و فعال‌سازی تجهیزات تهیه نسخه پشتیبان و بازگردانی آن
- بازگردانی سیستم‌عامل‌ها و نرم‌افزارهای مهم مرتبط با سرویس
- روش تست عملیاتی و تست امنیت سیستم‌های بازگردانی شده
- روش اتصال سیستم به شبکه و تجهیزات دیگر.

❖ فاز بازسازی (Reconstitution)

این فاز، در واقع بازگشت به وضعیت تجهیزات و سرویس‌ها قبل از وقوع حادثه است؛ بدین معنا که تجهیزات و سرویس‌ها به مرکز داده بازگشته است و اکنون می‌بایست سرویس به وضعیت معمول قبل از حادثه بازگردد.

پس از فاز عملیات و اتمام بازگردانی سرویس به حالت اولیه، فاز بازسازی برحسب اندازه و مقدار حادثه ممکن است از یک ساعت تا چندین روز به طول انجامد. در این فاز، پس از تعمیر تجهیزات یا حل مشکلات سرویس‌ها، سرویس به حالت قبل از عملیات بازگردانی بازخواهد گشت. در این فاز، موارد ذیل می‌بایست مدنظر قرار گیرد:

- مانیتورینگ و پایش تجهیزات و سرویس‌ها پس از انجام تعمیرات و تغییرات
- اطمینان از عدم وقوع مجدد حادثه یا تهدیدات دیگر قابل وقوع
- اطمینان از عملکرد صحیح تمام سرویس‌ها، تجهیزات و زیرساخت‌ها
- خاموش کردن سیستم‌های نصب شده یا راه‌اندازی شده جدید
- پایان دادن به فعالیت‌های اضافی در جهت بازیابی
- بازگردانی کامل سرویس از سایت Disaster
- مدیریت نیروی انسانی در جهت بازگشت به تجهیزات و سرویس‌های اولیه و قبل از DRP.

۱۲ فرایند تست سرویس

فرایند تست سرویس می‌بایست بر اساس یک ساختار مشخص و مطابق با روش‌های ذیل انجام شود.

۱. تست بر اساس چک‌لیست

چک‌لیستی از موارد بااهمیت در حوزه بازگردانی سرویس می‌بایست تهیه شده و تمام موارد با اصل صحیح بودن بررسی گردند.

ردیف	چک‌لیست تداوم سرویس
۱	آیا مستندات بازگردانی نرم‌افزارها و سخت‌افزارها موجود است؟
۲	آیا مستندات بازگردانی نرم‌افزارها و سخت‌افزارها مناسب و کامل است؟
۳	آیا شماره‌های تماس افراد و شرکت‌های کلیدی موجود است؟

۴	آیا از اطلاعات به صورت برنامه‌ریزی شده، نسخه پشتیبان تهیه می‌شود؟
۵	آیا نسخ پشتیبان گرفته شده، تست شده و قابل بازگردانی هستند؟
۶	آیا فایل‌های پیکربندی تجهیزات، قابل بازگردانی است؟
۷	آیا اطلاعات پشتیبان گرفته شده، به خارج از مرکز داده انتقال و در محیط امنی نگهداری می‌شوند؟
۸	آیا کابل دوم برق تجهیزات موجود بوده و در صورت قطع کابل اول، کارکرد صحیح را دارد؟
۹	آیا SAN دارای کنترلر دوم بوده و کارکرد صحیح را دارد؟
۱۰	آیا نام‌های کاربری و کلمات عبور، در زمان وقوع حادثه جهت دسترسی به سیستم‌ها وجود دارد؟

۲. تست Walk Through

در این نوع تست، یک بخش از طرح تداوم سرویس مورد آزمون قرار می‌گیرد. البته قابل توجه است که به صورت اصولی برای ورود به این نوع تست می‌بایست چک‌لیست تست به صورت مناسب مورد بررسی قرار گرفته باشد.

۳. تست شبیه‌سازی شده

در این نوع تست، سعی می‌شود رخدادی که ممکن است منجر به قطعی سرویس شود، شبیه‌سازی شده و سپس به صورت عملی مورد بررسی قرار گیرد تا امکان تحلیل عملکرد بخش‌ها به صورت دقیق فراهم شود.

۴. تست‌های موازی

در این نوع تست، اطلاعات در سایت اصلی یا سایت گرم بازگردانده می‌شود. به صورت منطقی می‌بایست تمام اطلاعات تا لحظه شروع تست یکسان باشد.

۵. تست بر اساس قطع سرویس

در این نوع تست، کل سرویس برای مدت زمان مشخصی که کمترین تأثیر را بر کسب‌وکار شرکت داشته باشد، قطع می‌شود. به طور مشخص می‌بایست تمام ساختارها و فرایندهای برنامه‌ریزی شده به صورت صحیح عمل نمایند.

۱۳ اطلاعات نسخه‌های پشتیبان سامانه/ سرویس

پارامتر	توضیحات
نام فایل پشتیبان بر روی Storage	
آدرس فایل پشتیبان بر روی Storage	
نام فایل پشتیبان بر روی Tape	
نام فایل پشتیبان بر روی Tape	
نام یا لیبل Tape	
تاریخ آخرین تست بازیابی فایل پشتیبان	
محل نگهداری کدمنبع (Source) برنامه سامانه	
محل نگهداری آخرین نسخه (Version) سامانه (نسخه	

کامل قابل نصب)	
نوع پشتیبان‌گیری	
دوره زمانی پشتیبان‌گیری	

نام فایل	کد فایل	تاریخ آخرین ویرایش
لیست اطلاعات مورد نیاز جهت تهیه نسخه پشتیبان		
لیست سوابق کنترل نسخه پشتیبان		
لیست نسخ پشتیبان‌گیری شده		

مسئول	نام و نام خانوادگی	تلفن ثابت	تلفن همراه
مسئول پشتیبان‌گیری			
مسئول بازیابی فایل پشتیبان			
جایگزین مسئول بازیابی فایل پشتیبان			

۱۴ فرایندهای جایگزین

فرایند انجام کار در صورتی که به هیچ عنوان امکان بهره‌گیری از شبکه، سامانه اطلاعاتی و سرویس وجود نداشته باشد، به شرح زیر است:

۱۵ فرایند پاسخ به رخدادهای سایبری

برای هر یک از مخاطرات اعلام شده در بخش‌های بالایی این سند که ارزش ریسک آنها بالاتر یا مساوی عدد ۵ است، سناریوی مخاطره مربوطه به صورت کامل و گام به گام در قالب جداول زیر شرح داده شده است.

سناریوها بر مبنای جایگزینی اکتیو خدمات (HA) بوده و هدف این است که از به وقوع پیوستن این مخاطرات جلوگیری شود.

نمونه

حادثه: دسترسی غیرمجاز به سامانه/ سرویس (به دلیل دریافت اطلاعات خاص ناشی از عدم پیکربندی صحیح سامانه/ سرویس) نام فعالیت‌های مرتبط: تداوم فعالیت سامانه/ سرویس				
افراد مورد نیاز برای	امکانات لازم برای	فناوری‌های مؤثر در	داده‌های مرتبط با	افراد مرتبط با پاسخ به

بازیابی پس از اختلال (صلاحیت یا مهارت)	بازیابی پس از اختلال	تداوم فعالیت سرویس (دوره بازبینی فناوری)	فعالیت سرویس	رخداد و بازیابی حادثه
بر اساس جدول افراد مؤثر در تداوم سرویس	- بررسی و کنترل تمامی دسترسی‌ها به سامانه/ سرویس و حساب‌های کاربری مربوطه - غیرفعال‌سازی، بررسی مجاز بودن و اعمال مجدد دسترسی‌ها در صورت نیاز - آخرین نسخه به‌روز سامانه	راهکار و فناوری مورد استفاده برای احراز هویت کاربران (همچون اکتیو دایرکتوری، LDAP، IAM و PAM)، در صورتی که کاربران/ راهبران از طریق این فناوری‌ها به سامانه/ سرویس مذکور دسترسی دارند.	- لیست کاربران/ راهبران مجاز سامانه/ سرویس - فهرست پالیسی های اعمال شده از طریق سامانه‌های احراز هویت - راهنمای تنظیمات امن سامانه/ سرویس	بر اساس جدول افراد مؤثر در تداوم سرویس

فرایند پاسخ به رخداد و بازیابی پس از اختلال

تیم NOC مرکز داده باید پس از شناسایی حادثه مربوطه از طریق سیستم‌های مانیتورینگ و پیشگیرانه و همچنین مشاهده رفتار مخرب، از طریق مدیر مرکز داده با راهبر سامانه/ سرویس تماس برقرار نماید. کارشناس پشتیبان سامانه/ سرویس با هماهنگی با راهبر آن نسبت به شناسایی حادثه ایجاد شده اقدام می‌نماید. گزارش‌دهی حادثه ایجاد شده به اشخاص ذینفع مرتبط با سامانه/ سرویس توسط راهبر آن و با همکاری مدیر فناوری اطلاعات و ارتباطات شرکت صورت می‌پذیرد.

اقدامات پاسخ به رخداد و بازیابی پس از اختلال

اقدام‌های پیشگیرانه:

- پیکربندی صحیح و امن سامانه/ سرویس توسط راهبر آن
- کنترل دسترسی‌ها به سامانه/ سرویس و تعریف لیست کاربران مجاز
- پایش مداوم عملکرد صحیح سامانه/ سرویس توسط کارشناسان NOC و راهبر آن
- پایش عملکرد سامانه احراز هویت کاربران توسط راهبر سرویس مربوطه (در صورت وجود)
- تهیه مداوم نسخه پشتیبان از سامانه/ سرویس و پایگاه داده آن و نگهداری نسخ در مکان امن مناسب.

اقدام‌های تشخیص حادثه:

راهبر سامانه/ سرویس پس از آگاهی از رفتار غیرعادی در سامانه/ سرویس و ایجاد دسترسی‌های غیرضروری و نامجاز در آن لازم است در اسرع وقت، اقدام‌های زیر را انجام دهد:

- بررسی وضعیت سامانه/ سرویس و سرورهای آن و همچنین ترافیک خروجی سامانه/ سرویس
- بررسی و تحلیل لاگ‌ها به منظور شناسایی منشأ حادثه
- برقراری تماس با کارشناسان مربوطه و هماهنگی حضور جهت برطرف‌سازی حادثه

- اطلاع‌رسانی حادثه به مدیر امنیت شرکت.

مهار حادثه:

- رفع حادثه توسط کارشناسان مربوطه در اسرع وقت و در صورت نیاز، بازنگری و اعمال مجدد دسترسی‌ها.

بازیابی از حادثه:

- بررسی و غیرفعال‌سازی دسترسی‌های غیرمجاز ایجاد شده در سامانه/ سرویس
- راه‌اندازی مجدد سامانه/ سرویس و بازگرداندن وضعیت به حالت عادی توسط راهبر آن، با همکاری کارشناسان سامانه/ سرویس و مدیر مرکز داده (در صورت نیاز)
- گزارش حادثه ایجاد شده، توسط راهبر سامانه/ سرویس و مدیر مرکز داده به مدیر امنیت شرکت
- مدیر امنیت شرکت گزارشی از حادثه و اقدامات متعاقب آن به اطلاع مدیر فناوری اطلاعات و ارتباطات شرکت ارسال نماید.
- توسط مدیریت فناوری اطلاعات و ارتباطات، گزارشی از حادثه به واحد حراست ارسال گردد.

۱۶ تاریخ اجرا و به‌روزرسانی

این سند از تاریخ تصویب، معتبر و قابل اجرا می‌باشد. در صورت لزوم، بازنگری شده و حداکثر در فواصل زمانی سالیانه مورد بازبینی قرار می‌گیرد.

۱۷ پیوست‌ها

ندارد.