چک‌لیست اضطراری

برای محافظت از شبکه

در شرایط بحرانی

Falnic.com

در بحران‌هایی مثل قطعی و نوسانات شدید برق، اختلالات اینترنت یا حملات سایبری، زیرساخت شبکه شما در معرض خطر جدی قرار می‌گیرد.

این چک‌لیست، راهنمای سریع و جامع برای کاهش ریسک و حفظ پایداری سرویس‌ها در چنین شرایطی است.

Falnic.com

برق اضطراری و حفاظت فیزیکی

- بررسی سلامت UPSها و اطمینان از شارژ کامل باتری‌ها
- اطمینان از عملکرد صحیح ژنراتورها و سوئیچ خودکار به آن‌ها (Automatic Transfer Switch)
- جدا کردن تجهیزات حساس از منابع برق ناپایدار
- محافظت فیزیکی از رک‌ها و تجهیزات در برابر آب، آتش، گرد و غبار و لرزش

Falnic.com

تهیه نسخه پشتیبان (Backup)

- ذخیره نسخه‌های پشتیبان در مکان‌های جداگانه (Off-site) یا سرویس‌های ابری مطمئن
- انجام تست بازیابی (Restore Test) به صورت دوره‌ای برای اطمینان از قابلیت استفاده بکاپ‌ها
- رمزگذاری نسخه‌های پشتیبان جهت افزایش امنیت داده‌ها

Falnic.com

پایش (Monitoring) دقیق منابع

- فعال‌سازی اعلان‌ها و هشدارها برای CPU، RAM، دیسک، شبکه و سایر منابع حیاتی
- استفاده از ابزارهای پایش معتبر مانند LibreNMS، PRTG، Zabbix و غیره
- تعیین آستانه‌های بحرانی برای هشدار سریع در صورت بروز مشکل
- گزارش‌گیری منظم و تحلیل روند عملکرد تجهیزات

Falnic.com

بررسی امنیت شبکه

- اطمینان از فعال بودن و تنظیم صحیح فایروال‌های سخت‌افزاری و نرم‌افزاری
- به‌روزرسانی فوری فریمور، سیستم‌عامل و پچ‌های امنیتی
- محدودسازی دسترسی‌های ریموت (مثل RDP و SSH) فقط به IPهای مشخص و معتبر
- بررسی و تحلیل لاگ‌های مشکوک در روترها، سوییچ‌ها و سرورها به صورت منظم

Falnic.com

تست و مستندسازی ارتباطات حیاتی

- تهیه لیست کامل سرویس‌های حیاتی مانند DNS، DHCP، VPN، Active Directory
- بررسی سلامت خطوط ارتباطی و فعال بودن قابلیت Failover
- مستندسازی دقیق آدرس‌های IP، حساب‌های کاربری، Credentialها و ذخیره امن آن‌ها
- فعال‌سازی Redundancy و سیستم‌های افزونگی در صورت امکان

اطلاع‌رسانی داخلی

- ایجاد کانال ارتباطی فوری و اختصاصی بین تیم IT و مدیریت (مثلاً گروه تلگرام یا واتساپ)
- ارسال گزارش خلاصه وضعیت به پرسنل کلیدی و تیم‌های مرتبط
- اطلاع‌رسانی شفاف درباره سرویس‌های در دسترس و خارج از دسترس
- تعیین مسئول پاسخ‌گو در هر بخش برای تسهیل مدیریت بحران

آماده‌سازی برنامه بازیابی (Disaster Recovery)

- تعیین اولویت‌بندی بازیابی برای هر سرویس و سیستم
- داشتن چک‌لیست Disaster Recovery واقعی، مستندسازی شده و به‌روز
- استفاده از سرورهای جایگزین (Hot Standby و Cold Standby) یا سرویس‌های ابری به عنوان Backup
- مستندسازی کامل فرآیند بازیابی (Restore) سیستم‌ها و سرویس‌ها

حفظ امنیت فیزیکی و کنترل دسترسی

- قفل بودن رک‌ها و محدود کردن دسترسی به اتاق سرور فقط به افراد مجاز
- غیرفعال کردن دسترسی کارت‌های قدیمی و حساب‌های کاربری غیرضروری
- فعال بودن سیستم‌های دوربین مداربسته و مانیتورینگ تصویری
- ثبت دقیق ورود و خروج فیزیکی به اتاق‌ها و رک‌ها

Falnic.com

ارزیابی نهایی و آماده‌باش

- مرور سریع و منظم همه مراحل بالا و بررسی نقاط ضعف احتمالی
- تهیه گزارش جامع وضعیت شبکه و ارسال آن به تیم تصمیم‌گیرنده
- حفظ آرامش تیم، مستندسازی دقیق هر اتفاق برای بحران‌های آینده

Falnic.com

تاب‌آوری، نتیجه تصمیم‌های سنجیده
پیـــش از وقـــوع بحـــران اســـت.

فالنیک (ایران اچ پی)
Falnic.com