Daten-Backup und -Wiederherstellung

Diese Checkliste soll Organisationen dabei helfen, einen robusten Prozess für Daten-Backup und -Wiederherstellung zu etablieren und aufrechtzuerhalten.

Durch die Befolgung dieser Schritte stellen Sie sicher, dass Ihre Daten geschützt sind und die Wiederherstellung im Falle eines Vorfalls schnell und zuverlässig erfolgt.

 # 1. Backup-Anforderungen bewerten

☐ Kritische Daten und Systeme identifizieren, die ein Backup benötigen (z. B. Datenbanken, Dokumente, Anwendungsdateien).
☐ Akzeptable Wiederherstellungszeitziele und Wiederherstellungspunktziele festlegen.
☐ Compliance-Anforderungen für Daten-Backups bewerten (z. B. DSGVO, ISO 22301/27001).
☐ Den Umfang der Backups festlegen: Vollständige, inkrementelle oder differenzielle Backups.

 # 2. Backup-Lösungen auswählen

☐ Eine Backup-Lösung wählen, die den Anforderungen Ihrer Organisation entspricht (z. B. cloudbasiert, vor Ort, Hybrid).
☐ Sicherstellen, dass die Lösung Verschlüsselung für sichere Datenübertragung und -speicherung unterstützt.
☐ Backup-Speicherorte auswählen (z. B. Cloud-Speicher, externe Festplatten, netzgebundene Speicher).
☐ Skalierbarkeit und Kompatibilität mit bestehenden Systemen prüfen.

 # 3. Backup-Prozesse implementieren

☐ Einen Backup-Zeitplan definieren (z. B. täglich, wöchentlich, monatlich) basierend auf der Kritikalität der Daten.
☐ Backups, wo möglich, automatisieren, um manuelle Fehler zu reduzieren.
☐ Versionierung verwenden, um mehrere Backup-Kopien für kritische Dateien zu speichern.
☐ Warnmeldungen einrichten, um Backup-Erfolge oder -Fehler zu überwachen.

 # 4. Backups testen und validieren

☐ Regelmäßige Testwiederherstellungen durchführen, um sicherzustellen, dass Backups vollständig und funktionsfähig sind.

☐ Backups unter verschiedenen Szenarien testen (z. B. Datenbeschädigung, Ransomware-Angriffe).
☐ Die Integrität verschlüsselter Backups validieren.
☐ Testergebnisse überprüfen und Probleme umgehend beheben.

 # 5. Wiederherstellungsprozesse implementieren

☐ Schritt-für-Schritt-Wiederherstellungsverfahren für verschiedene Szenarien dokumentieren.
☐ Rollen und Verantwortlichkeiten für Mitglieder des Wiederherstellungs-Teams definieren.
☐ Sicherstellen, dass Wiederherstellungstools und Anmeldedaten im Notfall zugänglich sind.
☐ Den Wiederherstellungsprozess regelmäßig testen, um Effizienz und Geschwindigkeit zu messen.

#6 Backup-Daten sichern

☐ Alle Backup-Daten während der Übertragung und im Ruhezustand verschlüsseln.
☐ Multi-Faktor-Authentifizierung (MFA) verwenden, um den Zugriff auf Backup-Systeme einzuschränken.
☐ Backups an mehreren Standorten speichern, um Risiken zu minimieren (z. B. extern, Cloud).
☐ Zugriffserlaubnisse für Backup-Systeme regelmäßig überprüfen und aktualisieren.

 # 7. Backups überwachen und pflegen

☐ Protokolle und Dashboards einrichten, um den Backup-Status und die Leistung zu überwachen.
☐ Backup-Zeitpläne überprüfen und an sich ändernde Geschäftsanforderungen anpassen.
☐ Alte Speichermedien ersetzen, um Datenverluste zu vermeiden.
☐ Anzeichen für unbefugten Zugriff oder Manipulationen überwachen.

 # 8. Backup-Richtlinien überprüfen und aktualisieren

☐ Eine schriftliche Backup- und Wiederherstellungsrichtlinie für Ihre Organisation erstellen.
☐ Backup-Prozesse, RTO-/RPO-Anforderungen und Aufbewahrungsrichtlinien einschließen.
☐ Die Richtlinie jährlich oder nach wesentlichen Änderungen überprüfen und aktualisieren.
☐ Mitarbeiter über Backup-Verfahren und die Bedeutung der Datenwiederherstellung schulen.

Brauchen Sie beim nächsten Schritt Hilfe?

Wenn Sie zu einem dieser Schritte eine Frage haben oder Hilfe beim Einrichten einer fortgeschritteneren oder maßgeschneiderten Lösung benötigen, sind wir für Sie da!

Senden Sie uns einfach eine E-Mail an contact@403bits.com.

Bei einfacheren Fragen geben wir Ihnen gerne Ratschläge oder weisen Sie in die richtige Richtung – kostenlos!

Und wenn Sie vor einer komplexeren Herausforderung stehen oder Zeit sparen möchten, können unsere Experten übernehmen und eine umfassende Einrichtung bereitstellen, die perfekt zu Ihren Anforderungen passt.

Wir sind hier, um Ihnen beim Aufbau von Sicherheit und Effizienz zu helfen, damit Sie sich auf das Wachstum Ihres Unternehmens konzentrieren können!

Wenn Ihnen diese Checkliste gefallen ist oder Sie Verbesserungsvorschläge haben, lassen Sie es uns unter contact@403bits.com wissen.