RemoteDesk

Ultimate 20+ Point

Checklist for Data Protection & Security While Working Anywhere!

A proactive approach to Data loss protection

Get ready for breaches by learning why they happen and what makes costs go up or down. Check out our 2024 Data Protection and Security Checklist for easy tips. Listen to experts who've been there.

"Data breaches hit businesses across all sizes and sectors more frequently than you might realise. With the rise of remote and hybrid work, along with increased employee burnout and faster development cycles, oversight can slip and security habits weaken. This opens the door to new vulnerabilities, making it easier for data breaches"

Investing now can save Millions

$4.45 mn

This was the global average cost of a data breach in 2023, a 15% increase over 3 years.

$1.76 mn

This was the average savings for organizations that use security AI and automation extensively compared to organizations that don’t.

95%

of IT leaders say that data breaches are more sophisticated than ever.

82%

of breaches involved data stored in the cloud.

51%

of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

28%

of organizations used security AI extensively, which reduces costs and speeds up containment.

*Safeguarding your organization’s data is a constant battle with evolving threats. By investing in the right people, processes, and technologies, you can lower your risk and strengthen your security, bolstering your entire business. Use our data breach prevention checklist to proactively defend against security threats.

Data Protection and Security checklist*

☐ Review process for new tool/software:

- It helps reduce friction and make it easier for teams to get their work done with the tools they prefer. But, if they are using new tool/ software, make sure they know how to use those additional tools safely.

☐ Identity Verification:

- Implement continuous facial verification for employee identity, utilizing biometric authentication technologies (Face or ID verification).
- Implement 2-factor authentication / multi-factor authentication (2FA / MFA) for enhanced security, requiring additional factors beyond passwords for access.

☐ Presence Monitoring:

- Deploy activity monitoring tools to detect employee presence in front of systems handling sensitive data, and utilize automated prompts for identity confirmation before accessing PHI, PCI or other sensitive data.
- Utilize AI-based solutions to detect imposters and unauthorized access attempts.

☐ Access Controls:

- Implement Zero Trust policy for restricted access, assuming all network traffic is untrusted by default and verifying identity and authorization for every request.
- Enforce least privilege access controls, granting users the minimum level of access necessary according to their roles and responsibilities.

☐ Data Classification:

- Classify data based on sensitivity and importance, identifying and labelling data as PHI, PCI, PII, or other sensitive categories.
- Implement access controls and encryption based on data classification, applying stronger security measures to highly sensitive data.

☐ Data Encryption:

- Encrypt data at rest and in transit, utilizing encryption algorithms and protocols such as AES for data protection.
- Implement encryption for email communications containing sensitive information, ensuring secure transmission of sensitive data over email.

☐ Data Masking and Anonymisation:

- Implement data masking and anonymization techniques for non-production environments, protecting sensitive data used for testing or development purposes.
- Ensure that personally identifiable information (PII) is anonymized when not required for business processes.

☐ Data Loss Prevention (DLP):

- Implement DLP solutions to prevent unauthorized sharing or transmission of sensitive data, monitoring and controlling the movement of data across the network.
- Configure DLP policies to detect and block unauthorized access or data exfiltration attempts.

☐ Endpoint Protection and Security Tools:

- Deploy endpoint protection platforms (EPP) and encryption mechanisms, protecting devices against malware, ransomware, and other threats.
- Utilize intrusion detection systems (IDS) and prevention systems (IPS) for network security, detecting and preventing unauthorized access or malicious activities on the network.

☐ Identity and Access Management:

- Implement robust Identity and Access Management (IAM) solutions, managing user identities, access rights, and privileges centrally.
- Enforce role-based access controls (RBAC) and attribute-based access controls (ABAC), assigning permissions based on roles or specific attributes of users.

Incident Response and Monitoring:

- Develop and implement robust incident response procedures, establishing incident response teams and escalation procedures.
- Utilize Security Information and Event Management (SIEM) solutions for centralized log management, monitoring security events, detecting anomalies, and responding to incidents promptly.

Vulnerability Management:

- Implement a vulnerability management program, regularly scanning systems for security vulnerabilities and prioritizing patching and remediation efforts based on risk assessment.
- Utilize vulnerability assessment tools to identify weaknesses in software, configurations, and infrastructure components.

Secure File Transfer and Data Access Logging:

- Utilize secure protocols for file transfer, using protocols like SFTP or HTTPS for secure file transfer and implementing encryption for files containing sensitive data during transfer.
- Enable logging of data access and modification activities, monitoring and auditing access to sensitive data and implementing alerts for suspicious data access or modification attempts.

Data Backup, Retention, and Disposal:

- Establish regular data backup procedures, backing up critical data at regular intervals to prevent data loss and testing data recovery processes to ensure readiness for potential data breaches or disasters.
- Establish data retention policies based on regulatory requirements and business needs, defining retention periods for different types of data, and implementing secure data disposal procedures to securely delete or destroy data when no longer needed.

Continuous Monitoring and Compliance:

- Implement continuous monitoring solutions, tracking changes in system configurations, user activities, and access permissions, and conducting regular security audits and assessments to evaluate the effectiveness of security controls and identify areas for improvement.
- Ensure compliance with regulatory requirements such as HIPAA, PCI-DSS, and GDPR, regularly reviewing and updating policies and procedures to align with regulations, and reviewing and updating third-party contracts and agreements for compliance, ensuring that third-party vendors handling sensitive data adhere to security and privacy requirements.

User Behavior Analysis:

- Implement User Behavior Analytics (UBA) tools, analyzing user behavior patterns to detect anomalies and potential insider threats.
- Utilize machine learning algorithms for advanced anomaly detection.

Secure Development Practices:

- Incorporate security into the software development lifecycle (SDLC), conducting secure code reviews and vulnerability assessments during development.
- Implement secure coding practices to prevent common vulnerabilities such as injection attacks or insecure authentication mechanisms.

Data Privacy Training and Awareness:

- Provide data privacy training and awareness programs for employees, educating them on the importance of data security and privacy and raising awareness about common threats such as phishing attacks or social engineering tactics.

Secure Collaboration:

- Deploy secure collaboration platforms for remote work, ensuring encryption of communications and data sharing, and conducting regular security assessments of collaboration tools to ensure compliance with relevant regulations and industry standards.

Regularly review your security plan:

- Security risks are always evolving. You need to adjust your strategy as your company scales and transforms to keep pace with the changing security landscape. Create a process that allows you to consistently review your security measures so you’re not caught with outdated practices.

RemoteDesk, is a trusted partner to revolutionize the way organizations safeguard their sensitive information and ensure compliance in today's dynamic work environment. It specializes in providing advanced solutions that leverage the power of Computer Vision AI to address the evolving challenges of remote work and data protection. Our comprehensive suite of services is meticulously crafted to meet the unique needs of modern businesses.

* **This provides a broad overview of preventive measures to secure your business. Remember, there's no one-size-fits-all security solution, so not everything listed here may apply to your specific situation.**

Next Steps

See how we can leverage RemoteDesk in your Environment.

Schedule a Demo:

Contact Us:

+1-773-8392840
pr@remotedesk.com