Salesforce Cybersecurity Health Checklist

EzProtect
By Adaptus

Salesforce Cybersecurity Health Checklist

EzProtect By Adaptus

As a trusted Salesforce partner, EzProtect has put together this helpful cybersecurity health checklist to make sure there are no gaps or vulnerability points. Use our basic Salesforce cybersecurity health checklist so you can minimize risks wherever possible to keep your system and your reputation secure:

- [ ] **Require all frequent updates of virus protection and other software on employee-issued technology**
  This ensures you have the latest protections baked into your computers and prevents any loopholes from staying open.

- [ ] **Regularly backup all data your company stores on Salesforce.**
  One of the key defenses to a ransomware attack is having current backups of your data. This ensures that you can quickly and easily restore data in the event of an attack.

- [ ] **Implement a complex password policy.**
  A regular cadence for changing passwords and setting robust password requirements (capital letters, symbols, numbers, etc.) keeps your systems safer and your data more secure.

- [ ] **Require VPN access for all employees that log in to Salesforce.**
  VPN access is key to securing your network, giving you a higher level of control of who can access company data. Whitelisting your company IP addresses is a must—preventing users who are not connected to VPN from logging into Salesforce.

  If employees are working from home, they must log in to the company VPN to connect from one of those whitelisted IP's. Otherwise, they must log in from a company office. This makes it easy to spot IP addresses you don't recognize that may be accessing your data, saving you time and resources from having to shoot down threats as they pop-up.

  BE SURE to require employees to stay logged into your VPN once they are logged on to Salesforce, otherwise they may bypass your network virus scanning gateways, making them vulnerable to malware and hackers.

- [ ] **Set up Salesforce multi-factor authentication.**
  VPN access is key to securing your network, giving you a higher

  By opting in to Salesforce's two-factor authentication, you set strict parameters for who can access your Salesforce data and when they can access it.

- [ ] **Scan for viruses.**
  If your company uploads and downloads files from Salesforce, consider adding a software that scans these files for viruses. Add EzProtect by Adaptus to take the guesswork out of virus scanning on your Salesforce system.

- [ ] **Conduct audits to ensure compliance with cybersecurity best practices are up to date.**
  Auditing gives your team peace of mind that all cybersecurity best practices are up to date and properly adhered to. It also allows for self-reflection on where your team can improve.

  By regularly checking who accesses your data and when, you can better identify irregular patterns of access. Create a cadence for pulling these reports and promptly review them to make sure all user access levels are what you expect.