SaaS Security Checklist

Modify this checklist according to your needs. Check ‘Yes’ if the policy, feature, or functionality is available and properly set. Check 'No' if any aspect is missing or not entirely fulfilled.

Data Security & Threat Detection Framework

Are the following security strategies implemented?		
• Multi-factor authentication techniques	☐ Yes	☐ No
• Encrypted data in transit and at rest	☐ Yes	☐ No
• Access controls and least privilege principles	☐ Yes	☐ No
• Routinely assessed user data access for compliance	☐ Yes	☐ No
• Effective DLP solutions	☐ Yes	☐ No
• Systematic monitoring for common threats	☐ Yes	☐ No
Do you understand the potential risks connected with each provider's integration points?	☐ Yes	☐ No
(Other)	☐ Yes	☐ No

Compliance

Are these audits and assessments regularly performed by trained personnel?		
• General Data Protection Regulation (GDPR)	☐ Yes	☐ No
• ISO 27000 standards	☐ Yes	☐ No
• Systems and Organization Controls (SOC)	☐ Yes	☐ No
• Payment Card Industry Data Security Standard (PCI DSS)	☐ Yes	☐ No

This is a sample SaaS security checklist from esecurityplanet.com.
Feel free to customize this template to fit your organization's specific requirements and context.

• NIST 800-53 Risk Management Framework	☐ Yes	☐ No
(Other)	☐ Yes	☐ No
Vendor Evaluation		
Does your SaaS vendor and their solution provide the following?		
• Dedicated customer support	☐ Yes	☐ No
• Measured and monitored uptime and responses	☐ Yes	☐ No
• Automated monthly reporting features	☐ Yes	☐ No
• Integrations with other SaaS applications, platforms, or single sign-on solutions	☐ Yes	☐ No
• References or case studies of successful security implementations	☐ Yes	☐ No
• Clear terms and conditions of the contract, including renewal alerts, termination clauses, and data ownership rights	☐ Yes	☐ No
• Automated SaaS security monitoring and alerts	☐ Yes	☐ No
(Other)	☐ Yes	☐ No
IT Infrastructure Analysis		
Have you performed or deployed the following?		
• Regular penetration tests and security tests to check for vulnerabilities	☐ Yes	☐ No
• Firewalls to protect against unauthorized access and data breaches	☐ Yes	☐ No
• Intrusion detection systems to monitor unusual activities	☐ Yes	☐ No
• Access controls to manage user permissions	☐ Yes	☐ No
Have you removed the unused and unnecessary	☐ Yes	☐ No

This is a sample SaaS security checklist from esecurityplanet.com.
Feel free to customize this template to fit your organization's specific requirements and context.

software and devices from the infrastructure?		
Do you consistently use secure protocols and channels for all communications?	☐ Yes	☐ No
(Other)	☐ Yes	☐ No
Cybersecurity Training		
Have you tested and deployed a secure cybersecurity training tool?	☐ Yes	☐ No
Have employees been informed of the following?		
• Risky cybersecurity behaviors, such as accessing public Wi-Fi or unsecured personal devices	☐ Yes	☐ No
• Cybersecurity best practices, including setting strong passwords in accordance with the organization's policy	☐ Yes	☐ No
• Basic security risks like malware, phishing, and hardware loss	☐ Yes	☐ No
• Strong authentication techniques	☐ Yes	☐ No
Are staff routinely assessed on their cybersecurity knowledge and awareness using tests or simulations?	☐ Yes	☐ No
(Other)	☐ Yes	☐ No
Disaster Response		
Do you have a designated incident response team?	☐ Yes	☐ No
Have you defined a disaster response strategy describing specific processes for dealing with various types of incidents?		
• Clearly established roles and duties	☐ Yes	☐ No
• Set procedures to facilitate communication during and after a disaster	☐ Yes	☐ No
• Documented lessons learned with tested and updated response strategy	☐ Yes	☐ No

This is a sample SaaS security checklist from esecurityplanet.com.
Feel free to customize this template to fit your organization's specific requirements and context.

• Contingency plans for business continuity	☐ Yes	☐ No
(Other)	☐ Yes	☐ No
Policy Evaluation & Updates		
Have you documented, addressed, and updated the following?		
• Formal framework for conducting retrospective analysis of cyber incidents	☐ Yes	☐ No
• Gaps and lessons learned	☐ Yes	☐ No
• Security processes, procedures, training, and policies	☐ Yes	☐ No
Is there a dedicated person or team in charge of overseeing the updating process?	☐ Yes	☐ No
Are security updates successfully disseminated to important stakeholders?	☐ Yes	☐ No
Are there systems in place to track and monitor the deployment of modifications to guarantee consistency?	☐ Yes	☐ No
(Other)	☐ Yes	☐ No