Customer Security Questionnaire Common Questions

Question	Answer
SOC2 Compliance	Type 1 completed and Type 2 expected by EOY 2019
Access Logging -Log of success/failure attempts with Polly Application	We rely on Slack for login via OAuth and in fact don't receive any identifiable information if the login is unsuccessful. Slack has the ability to show login attempts on their admin panel.
Traffic Logging	We don't currently log IP addresses of activity happening in our app due to GDPR. However, should a customer opt into our single tenancy tier, this can be enabled for that environment. Additionally, Slack also shows all IP addresses that have accessed a workspace on their premium tiers.
Action Logging	We allow exports from within the application for activity logs. This is available to administrators on our Enterprise tier.
Code Scanning	Yes, we do perform automated code scans as well as manual code inspections for security strengthening.
Intrusion Detection/Prevention	Yes, we use Amazon GuardDuty to monitor our production environments in AWS for any untoward activity.
Vulnerability Scanning/Patch Management	Yes, we perform regular patching of all key dependencies and perform routine audits to ensure that we're up to date.
Anti-Malware / Anti-Virus	Yes, all company laptops are required to have anti-malware running. We are also putting into place a system for malware scans on production images before deployment.
Incident Response (Security issues)	Yes, we have a documented incident response policy and it requires customer notification.
Data Encryption	Data at rest in our database is encrypted with EBS SHA-256 block level encryption. Data in transit is encrypted with TLS 1.1+ (HTTPS) by our edge servers and to our database
Data Isolation, Retention & Destruction	Data isolation i.e. single tenancy is an optional upgrade that can be purchased for the company's license. By default, Polly operates on a shared tenancy model. Custom retention policies are available with our Enterprise plan. Data can be removed upon request at any time.
Data Privacy	We take data privacy very seriously and are compliant with EU/US Privacy Shield and GDPR
Single-Sign On (SSO) Multifactor Authentication (MFA)	We offer SSO through Slack and inherit the MFA setting therein.
IP Source Whitelisting	N/A - MFA possible through Slack
Role Based Access Controls (RBAC)	We allow users only access to their own data or to users data that has been explicitly shared to them. Additionally, we offer an additional administrator role with our enterprise plan that can access and set policies for data across the organization.
Data Classification strictly confidential, confidential, restricted, or unrestricted?	Restricted
Data Compromised Impact	The intruders would be able to find out the content of the polls. We do not intend to put any confidential or strictly confidential information into the polls. Intruders would be able to get a list of Slack users, names, and email addresses
Data Centers ISO 27001	We rely on Amazon AWS: https://aws.amazon.com/compliance/iso-27001-faqs/
Payment card data centers certification	We rely on Stripe for payment processing which is a PCI Level 1 service provider https://stripe.com/docs/security/stripe
Insurance Policy	We carry a general business insurance policy, along with cyber and E&O (errors and omissions) insurance

Security Incident Notification	We comply with the principles outlined in GDPR which requires notifications within 72 hours of discovery of impact. We would attempt to reconstruct what happened in any incident and take necessary measures to stop any active breach as well as recover data that might be impacted.
Continuity Plans	We have a documented business continuity plan and rely on our cloud providers to help maintain high availability and redundancy.
Dedicated Security Staff	We have a dedicated Security Engineer
Employee Confidentiality and Data Security training	Employees are required to perform annual security training, and must sign a security statement during onboarding
Protect against malicious internal employee	We conduct background checks on employees and maintain a system of least privilege access. Audits are conducted regularly of access to systems for employees.
E-Discovery	Available on Enterprise level plans
Geographic Data location	United States
Allow customer to perform audit of data	This is not possible due to our shared tenancy model. Note that we can offer a single tenant solution hosted on AWS at a higher cost.
Workstation Security Monitoring	All workstations are managed through MDM software. Workstations require automatic idle lock screens after 5 minutes. Workstations require full disk encryption.
Production Security Monitoring	AWS environment including servers, load balancers etc. are continuously monitored using GuardDuty
Operating systems and software applications refreshed and updated regularly	Yes
Network URL filtering	No: Mitigated through MDM software and malware scanning
Data loss prevention solution	Yes
Store sensitive data in server logs	No: Information is scrubbed from logs
Perform code reviews	Yes
Perform user account reviews to systems	Yes, we perform quarterly reviews of access to all systems
Is penetration testing performed regularly	Yes: Penetration testing results can be provided separately