Compliance requirements for Out-sourced Services

Assumption:

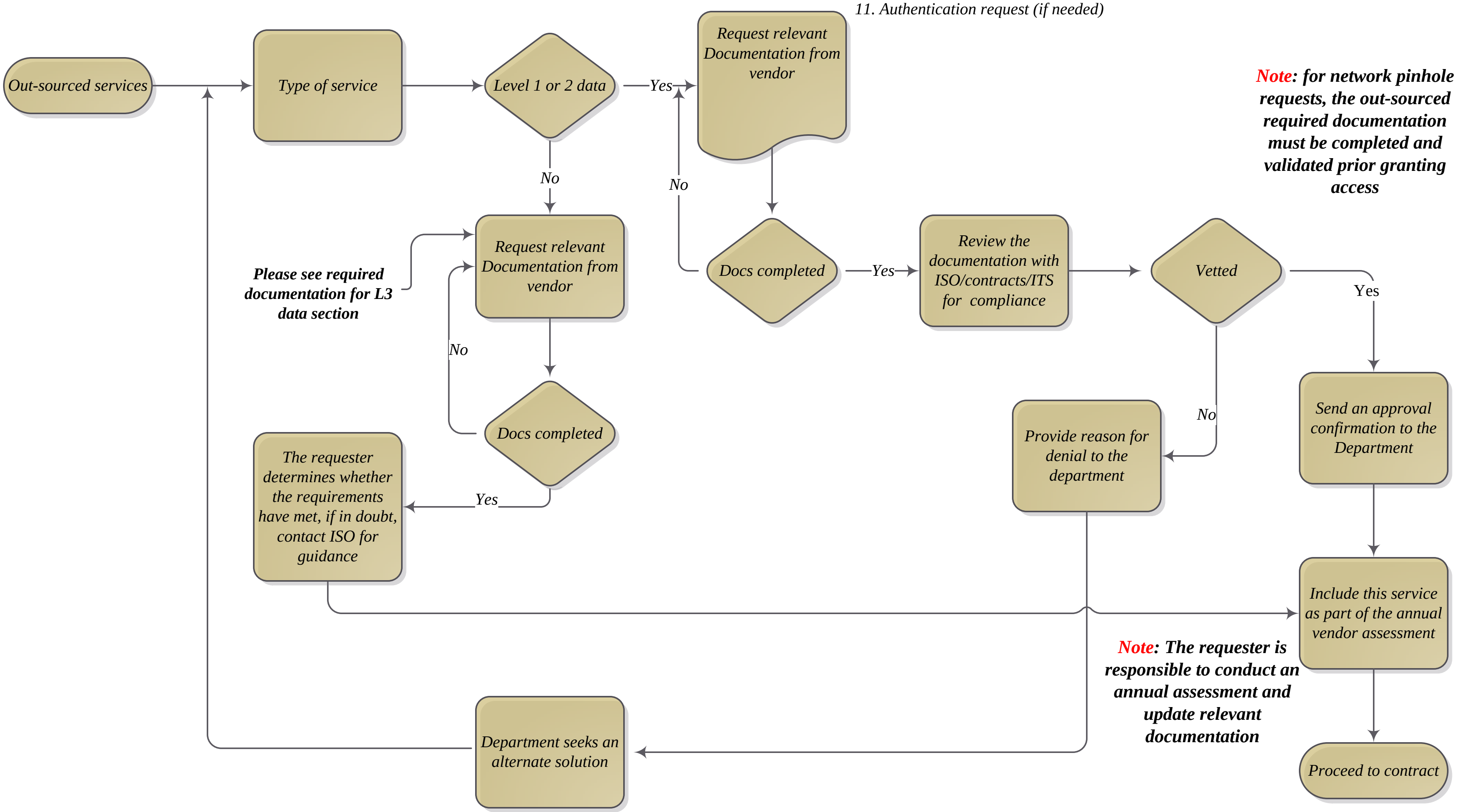
- *The requester (service owner is a Cal Poly unit/employee) is responsible for meeting all applicable policies, standards or regulations.*
- *Must provide all the required documentation*
- *This requirement applies to any third party service provider*

Required documentation for L1 or L2 data

1. Attestation of Compliance (AOC) – (e.g. cert from Cloud Security Alliance)
2. Report on Compliance (ROC) – (SOC3, SSAE16)
3. Contract (confidentiality agreement)
6. Dataflow
7. Third-Party Vendor Security Questionnaire (CSA V3 questionnaire for Level 1 data Cal Poly questionnaire for level 2 data)
8. Incident Response (this should be included in the contract)
9. Security exception (if needed)
10. Application data request (if needed)
11. Authentication request (if needed)

Required documentation for L3 data

1. Contract
2. Third-Party Vendor Security Questionnaire (Cal Poly – 45+ questions)
3. Security exception (if needed)
4. Application data request (if needed)
5. Authentication request (if needed)


Out-sourced services
Type of service
Level 1 or 2 data
Yes
No
Request relevant Documentation from vendor
No
Docs completed
Yes
Review the documentation with ISO/contracts/ITS for compliance
Vetted
Yes
No
Request relevant Documentation from vendor
No
Docs completed
Yes
The requester determines whether the requirements have met, if in doubt, contact ISO for guidance
Provide reason for denial to the department
Send an approval confirmation to the Department
Include this service as part of the annual vendor assessment
Department seeks an alternate solution
Proceed to contract

Please see required documentation for L3 data section

Note: for network pinhole requests, the out-sourced required documentation must be completed and validated prior granting access

Note: The requester is responsible to conduct an annual assessment and update relevant documentation