Cloud Security Questionnaire

This questionnaire is intended to capture security information regarding cloud services utilized by the City of Charlotte. The form should be filled out by a City employee along with the provider of this cloud solution (vendor). Completed forms may be submitted for review by a City employee via the Cloud Security Review form on the City's self-service portal.

Note: Question 1 through Question 14 must be answered by a City of Charlotte employee or contractor.

#	Question	Answer
1	Please describe this cloud solution and how it will be used by the City of Charlotte. What problem does this cloud solution solve?	
2	Which City departments plan to use this solution?	
3	Which City users plan to use this solution? How many users? Which users will administer this solution?	
4	Will this cloud solution connect to current systems inside the City's network? If yes, please provide an architecture diagraming showing this connectivity.	
5	Will any computing devices (servers, workstations, IoT, etc.) be added to the City's network as a part of implementing this cloud solution?	
6	What types of data will this cloud solution store or process?	
7	Will this cloud solution store or process payment card data (i.e. PCI data)? If so, please provide evidence of Attestation of Compliance (AoC).	
8	Will this cloud solution store or process Protected Health Information (PHI)?	
9	Will this cloud solution store or process Personally Identifiable Information (PII)[i]? If yes, which types of PII?	
10	Will this cloud solution store or process Criminal Justice Information (CJI)?	
11	Will this cloud solution store or process any other type of restricted data as defined in the City's Protection of Restricted Data policy (ADM 13)?	
12	Will this cloud solution store or process any other sensitive or confidential data not identified above?	
13	For the data types listed above, what are the sources of the data and what processes and protocols are used upload the data into this cloud solution?	
14	If a bad actor found a way to compromise this cloud solution and was able to tamper with, delete, and/or leak the data it will store or process, what is the possible impact to City operations and reputation?	
15	What methods does this cloud solution use to send/transfer City data out to other systems?	

16	Does the vendor have cyber liability insurance? If yes, does the vendor’s insurance cover City of Charlotte assets and data in the event of a breach?	
17	Has this cloud solution (*not* the hosting provider) been ISO 27001 certified? If “yes”, please provide proof of certification.	
18	Is this cloud solution (*not* the hosting provider) FedRAMP authorized? If “yes”, please provide proof of authorization and Impact Level (Low, Moderate, or High).	
19	Has this cloud solution (*not* the hosting provider) undergone a SOC 2 audit? If “yes”, please provide proof of audit.	
20	What encryption algorithms does this cloud solution use to encrypt Data At Rest (DAR encryption)?	
21	What encryption algorithms does this cloud solution use to encrypt Data In Transit (DIT encryption)?	
22	How does the vendor manage encryption keys for this cloud solution?	
23	Who has access to the cloud solution’s encryption keys?	
24	For both data stored in this cloud solution and backups, in which countries will the City’s data be stored?	
25	Does this cloud solution support federation with Okta for Single Sign-On (SSO) authentication using Security Assertion Markup Language (SAML)? If “no”, please describe this cloud solution’s user password policy and two-factor capabilities, including any customer-controlled options.	
26	Please describe the vendor’s vulnerability management program.	
27	Does the vendor have a third-party perform yearly penetration tests on this cloud solution and when was the most recent penetration test completed?	
28	Who can see or have access to the City’s data stored, processed, or transmitted by this cloud solution?	
29	How does the vendor safeguard the City’s data from other customers and prevent unauthorized viewing of the City’s data?	
30	Is this cloud solution hosted on a dedicated or shared instance/infrastructure?	
31	Please describe the vendor’s security Incident Response (IR) process.	
32	What is the timeline for customer notification in the case of a breach?	
33	What activities/actions within this cloud solution are logged?	
34	How does the vendor allow customers to view audit and access logs?	

35	How does the vendor communicate with customers about important changes to the vendor's platform or processes?	
36	Does the vendor offer periodic reports confirming compliance with security requirements?	
37	What happens to the City's data when service is terminated?	
38	Describe the process the vendor uses to destroy data after customers release it?	
39	Please describe the vendor's backup process.	
40	How many backups of the City's data are stored, where are they stored, and are they encrypted?	
41	Please describe the vendor's Disaster Recovery (DR) processes.	
42	What is the vendor's current uptime and Service Level Agreement (SLA) option?	
43	How does the vendor screen employees and contractors?	
44	What cloud/hosting service hosts this cloud solution? If this cloud solution is hosted on Amazon Web Services (AWS), Google Cloud (GCP), or Microsoft Azure, the questions listed below can be skipped.	
45	What is the vendor's process for responding to a legal hold request?	
46	What certifications for the data center have been achieved?	
47	Where is the vendor's data center and what physical security measures are in place?	
48	How does the vendor dispose of End-Of-Life (EOL) hardware?	
49	How does the vendor dispose of failed data storage devices?	

[i] The following types of Restricted Data constitute PII: social security numbers, employer taxpayer identification numbers, drivers' license numbers, state identification card numbers, passport numbers, checking account numbers, savings account numbers, credit card numbers, debit card numbers, personal identification code (PIN) numbers, digital signatures, any other numbers or information that can be used to access a person's financial resources, biometric data, fingerprints, and passwords.