|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Cloud** | **Datacenter** | **Endpoint Device** | **IoT Device** |
| **Data**  Yes or No  or both with conditions | Yes or No  PII, PCI, PHI, Financial Data (FD) and Intellectual Property (IP) | Yes or No  PII, PCI, PHI, FD, IP | Yes or No  PII, PCI, PHI.  Senior Staff by segment – Yes FD and IP | Yes or No  PII, PCI, PHI, FD, IP |
| **Application**  Keep, add, or subtract as needed | Financial  Staff Training  Payroll  Email  Grading  Meals  Transportation  Website  Ed Material  Gov Data Reports | Access Control  Camera  HVAC  Data Backup  Data Archive  Phones | Grading Portal  Customer Portal  Training Portal  Payroll Portal  Email | POS  RFID Readers  Camera  Keypad Readers  Security Portal  Camera |
| **Assets**  Keep, add, or subtract as needed | Third Party – pay by the contract term for server usage  Backup server | AD Server  VEAAM Server, Firewall  Phone Server | Desktop Computers, Laptops, Tablets, Phones, BYOD, Central Printer | POS  RFID Readers,  Camera  Keypad Readers,  Security Portal |
| **Services**  List the business services in order 1 to # |  |  |  |  |

**Pick a business process and list every way the system can be breached.**

* Third-party IT representative loses the endpoint device in transport with all data on the device.
* Device with data was stolen from the staff personal vehicle.
* Rogue third-party IT employee regularly removes data and sells it.
* School or third-party IT past and present employees have access to the data and downloads it to sell it.
* New employee that receives a device can recover the data from the previous user and uses it for their purposes.
* Customer who purchased a device through e-commerce calls you and says they have your data.