*****The following are controls that must be in place for datacenters containing high or very high-risk information**

Controls	Very High risk/ High Risk Information	Has this been Completed?
Rooms	Datacenter must be located in a fully enclosed room where walls must extend from floor to ceiling slap and if not solid (e.g. Drywall), they must be reinforced with wire mesh.	Yes / No
Doors and Locks	Datacenter doors must be locked when room is not in use and the security grade door fastening hardware must be used in conjunction with a metal door and frame.	Yes / No
Glazing	All exterior glass in doors and accessible windows must be reinforced.	Yes / No
Managing Access	The public must not have direct access to the datacenter perimeter as only individual(s) with assigned authority to can grant access; someone must also be appointed to formally manage the physical access and it must be logged in a way that does not uniquely identify the individuals.	Yes / No
Alarms and Remote Monitoring	Alarms (monitored 24/7) must be installed that trigger on unauthorized access.	Yes / No
Environmental Controls	Sufficient Heating, Ventilation and Air Conditioning (HVAC) systems must be in place to effectively maintain, monitor and detect any variations all UBC Electronic systems within the manufacturers' required temperature and humidity operating ranges.	Yes / No
Fire Protection	Fire detection and suppression devices, such as fire extinguishers and pre-action or dry pipe sprinkler systems, must be in place.	Yes / No
Data Backups	If information is backed up onto electronic media, the same physical security requirements are to be applied to that media unless the information is encrypted (see the Encryption Requirements standard).	Yes / No

******For more information: https://cio.ubc.ca/information-security-standards/M9**