Physical Security

Toppan Merrill takes an aggressive stance on physical security at our locations and is backed by the strength of ISMS ISO/IEC 27001:2013 certification. ISO 27001 is designed to ensure the selection of security controls that protect information assets and provide a high level of confidence sought by the companies that partner with us or otherwise trust us to execute their critical business functions. With ISO 27001 framework in mind, Toppan Merrill ensures our physical security design incorporates reasonable and appropriate measures to prevent unauthorized access to facilities and to protect employees working within.

Power, Fire and Maintenance

- Backup generators and Universal Power Supplies (UPS) are available for critical functions and tested regularly to ensure minimal interruption should the need arise.
- Fire suppression matches the unique needs of its environment, factoring in the type of equipment present it is intended to control and based on local fire code regulations.
- Equipment is maintained per recommended service intervals and specifications with only authorized personnel carrying out repairs and servicing. Most maintenance efforts or building modifications are documented and logged for review with a requirement to document work performed on any security-related change (involving cameras, door locks or access controls, barriers, windows, etc.).

Cameras, Monitoring and Alarms

- Cameras monitor physical entry points as well as access to secure facility areas. They are placed to prevent tampering/disabling while ensuring a legible image for identification can be made and are reviewed periodically to ensure functionality. Footage is kept for several months' time.
- Standalone facilities have alarm systems monitoring all entrances and they are monitored for alerts by an outside agency or security guards on premise monitoring during and outside regular working hours.

Delivery, Third Party and Visitor Access

- Physical access for individuals is limited to areas necessary to perform tasks and is controlled with unique keys, keycards, or other badging systems.
- Detailed physical access logs for building access and secure area access (datacenters, restricted computing rooms, restricted media handling areas, etc) are kept and available for review.
- Before entering Toppan Merrill facilities, Third Parties' support personnel must conform to requirements of Toppan Merrill's information protection policy and are required to have documented authorization for access. These privileges are reviewed regularly to ensure business need aligns with an individual's functional role.
- Visitors are logged at first point of entry to Toppan Merrill facilities (logs are retained for review) and must provide proof of ID. They are given 1-day visitor badges and are escorted and supervised by authorized personnel.