Internal Security Regulations, public

Administrative accounts

The supplier maintains an always updated list of all employees of ELITS Global Group AB business group (from now on called ELITS) that have administrative rights within the provided public cloud environment (from now on called the service).
ELITS acknowledge providing that list to each customer of the service upon request.
There are no general accounts that have administrative rights, all accounts are individual, and all accesses are logged.
The administrative accounts of the service are limited to manage resource within the service, that does not have the privilege to log in to resources created by the customer.

Administrative access

All accesses to the service with administrative accounts are using a mix of user/password and individual certificates to authorize the administrator.

Internal review process of administrative accounts

Every third month, the Manager responsible for the service within ELITS, is required to do a manual review and approval of the list of issued administrative accounts.

Usage of administrative rights

The use of the administrative rights are restricted to system administration of the service.
Only upon request from the customer, and with the permission from the customer, the rights will be used to access resources within the service that are managed by the customer.
There are exceptions from this, listed under the Protective exceptions section below.

Protective exceptions

ELITS have the rights to use its administrative rights within the service to turn off/disable resources created by and managed by the customer to protect the service from damage.
Examples are, but not limited to, virus infected resources, hijacked resources or resources used for illegal purposes.
If such right is used, the customer will be informed on what has been done, why it has been done and what is required before the resource can be put online again.