

C L I F F O R D
C H A N C E





PHYSICAL SECURITY

PHYSICAL SECURITY




Clifford Chance is committed to protecting our people, assets, brands and reputation by ensuring we have an effective and robust approach to the management of physical security risks. Our aim is to satisfy our duty of care, provide security to those working for or with Clifford Chance, and support our stated vision to be the “global law firm of choice”. We expect our suppliers to have appropriate physical security controls in place and advise us immediately in the event of a security incident that could impact us.

Minimum standards:

 <p>Physical Security Management Review & Assessment</p>	<ol style="list-style-type: none"> The Supplier shall ensure that it has an effective physical security management programme in place to support the identification and management of physical security risks to its organisation. The Supplier shall ensure that a security risk assessment, including physical security, is undertaken on an annual basis and any identified gaps are built into a remediation plan. 																																	
 <p>Physical Controls & Access & Oversight</p>	<ol style="list-style-type: none"> The Supplier shall ensure that appropriate and effective access control policies, procedures and systems are documented for all its personnel, and will be available for review by Clifford Chance. The Supplier shall ensure that all visitors, including third parties, temporary employees, contractors and clients) follow a designated site visitor process. The Supplier shall ensure that appropriate physical restrictions are deployed to detect, monitor and identify unauthorised access and security incidents. Example measures, include, but are not limited to: <table border="0" data-bbox="359 1064 1476 1433"> <tr> <td>External:</td> <td>Internal:</td> <td>People:</td> </tr> <tr> <td>a) Gates</td> <td>a) CCTV</td> <td>a) Clear Desk Policy</td> </tr> <tr> <td>b) Bollards</td> <td>b) Card Access Systems</td> <td>b) Staff Awareness and Vigilance</td> </tr> <tr> <td>c) Lighting (internal and external)</td> <td>c) Biometrics</td> <td>c) Pre-Employment Checks</td> </tr> <tr> <td>d) Fencing</td> <td>d) Infra-red Detection</td> <td></td> </tr> <tr> <td>e) CCTV</td> <td>e) Lockable Cabinets</td> <td></td> </tr> <tr> <td>f) Barriers</td> <td></td> <td></td> </tr> <tr> <td>g) Building Card Systems</td> <td></td> <td></td> </tr> <tr> <td>h) Biometrics</td> <td></td> <td></td> </tr> <tr> <td>i) Turnstiles</td> <td></td> <td></td> </tr> <tr> <td>j) Guarding</td> <td></td> <td></td> </tr> </table> Any equipment used by the Supplier shall conform to industry standard in terms of installation, operation, monitoring and maintenance. Images and data on CCTV must be stored in secured and restricted areas and be searchable by date and time. Any images or data on CCTV should be retained for a minimum of 30 days or in line with local laws/ regulation and be monitored by appropriately trained ‘Security Managers’, who will support the mitigation and management of identified security incidents or risks. 	External:	Internal:	People:	a) Gates	a) CCTV	a) Clear Desk Policy	b) Bollards	b) Card Access Systems	b) Staff Awareness and Vigilance	c) Lighting (internal and external)	c) Biometrics	c) Pre-Employment Checks	d) Fencing	d) Infra-red Detection		e) CCTV	e) Lockable Cabinets		f) Barriers			g) Building Card Systems			h) Biometrics			i) Turnstiles			j) Guarding		
External:	Internal:	People:																																
a) Gates	a) CCTV	a) Clear Desk Policy																																
b) Bollards	b) Card Access Systems	b) Staff Awareness and Vigilance																																
c) Lighting (internal and external)	c) Biometrics	c) Pre-Employment Checks																																
d) Fencing	d) Infra-red Detection																																	
e) CCTV	e) Lockable Cabinets																																	
f) Barriers																																		
g) Building Card Systems																																		
h) Biometrics																																		
i) Turnstiles																																		
j) Guarding																																		

PHYSICAL SECURITY

(CONTINUED)

 <p>Training</p>	<p>1. The Supplier shall ensure that all of its personnel receive training in terms of awareness of their own personal security, what to do if they experience a major incident, including their responsibilities. This should include, but is not limited to, site evacuation plans, alarms, etc.</p>
 <p>Travel</p>	<p>1. The Supplier shall ensure a duty of care is exercised over the security of its colleagues travelling internationally and follow the minimum standards outlined in our 'Travel and Expense Management Policy'.</p>
 <p>Processes & Procedures</p>	<p>1. The Supplier will have in place processes and procedures to manage security incidents and investigations, and provide an immediate update to Clifford Chance in the event any of Clifford Chance's information and assets could be impacted.</p>

CLIFFORD CHANCE

Document Owner: Procurement

Approved By: Director of Procurement & Chief Risk & Compliance Officer

Date Approved: 16th September 2020

Date for Review: September 2021

Version: 1.0

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2020

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

WWW.CLIFFORDCHANCE.COM