

Issue	Recommendations
Doors & Hardware	<p>Steel doors with industry standard security measures are recommended for all perimeter access points. Include the installation of strike/jamb pry protection and non-removable pin (NRP) hinges on all exterior doors where hinges are exposed to tampering from the building exterior. Ensure self closers function to shut and latch doors reliably under all building air pressure conditions.</p> <p>Aluminum door systems are particularly prone to prying attacks and should be installed with adeq</p> <p>In cases of extensive hardware deficiencies, contact the UBC Locksmiths Shop. They may work with a qualified Architectural Hardware Consultant (AHC) to develop recommendations for repairs or installation of new hardware.</p>
Key Control & Access Management	<p>Key control is a critical element of access control and contributes directly to Crime Prevention. Maintain strict control over all keys and report any missing keys to Campus Security.</p> <p>The Abloy Key System provides greatly enhanced protection and is highly recommended. Switching to Abloy keying can also provide the major advantage of regaining key control.</p> <p>Electronic Access Control systems can provide increased flexibility for managing access in larger or mixed user groups. Contact UBC Secure Access to inquire whether this option is applicable to your area or building.</p>
Electronic Security	<p>UBC Secure Access should be contacted to provide technical expertise on electronic security options, e.g. Alarm or Access Control systems and CCTV (Video Surveillance) installations. CCTV has been debated as an effective deterrent to crime, but if employed with adequate resolution and proper camera placement, its forensic effectiveness is undisputed. It leads to arrests and can lead to convictions, which take property criminals off the street.</p>
Glazing systems	<p>All exterior glass in doors and accessible windows should conform to high security standards. Consider installing high grade security film (minimum standard should be Profilon AXA1-15Mil or equivalent) to resist forced entry.</p>
Visibility of Assets	<p>Window coverings (blinds / shades) or reflective/tinted film should be installed on glazed windows or doors in order to reduce direct sightlines to valuables inside the facility. Staff should ensure these devices are in the closed position at the end of working hours. High-value assets such as iMac computers should be used in areas providing the least possible casual surveillance from public areas such as hallways, waiting rooms, etc. Any indicator lights or backlit Apple logos on equipment should be obscured from exterior view.</p>
Signage	<p>Use signage to clearly delineate publicly accessible space from Authorized Personnel-Only areas.</p>
Lighting	<p>Provide sufficient tamper-proof exterior lighting with unbreakable lenses to allow colour and facial recognition under low natural light conditions; apply lighting consistently to reduce 'light pooling' (minimize lighter/darker areas).</p>
Exterior Penetrations & Roof Access	<p>All exterior building penetrations should be protected against tampering and forced entry. Consider whether the roof provides access to the building. Consult Plant Operations and the Fire Department prior to implementing any security restrictions on roof access in order to ensure compliance with safety requirements.</p>