

## **MEMORANDUM**

**TO:** All Partners, Associates, and Support Staff

**FROM:** [Name/Management Committee]

**DATE:** [Insert Date]

**SUBJECT:** Directives for Securing Law Firm Premises

To ensure the safety of our personnel and the protection of confidential client information, the following security directives are effective immediately:

### **1. Access Control and Entry**

- All employees must use their issued key cards/fobs to enter the building.
- Do not hold doors open for individuals not recognized as firm employees.
- All visitors must sign in at the reception desk and be escorted by a staff member at all times.

### **2. Confidential Material Management**

- A "Clean Desk Policy" is in effect; all physical files and sensitive documents must be locked in cabinets at the end of each workday.
- Unauthorized removal of client files from the premises is strictly prohibited.
- Sensitive documents awaiting disposal must be placed in designated secure shredding bins.

### **3. Technology and Workstations**

- Computers must be locked (Windows + L / Control + Command + Q) whenever leaving the desk.
- The use of unauthorized external storage devices (USB drives) is prohibited.
- Any loss of mobile devices or laptops containing firm data must be reported to IT immediately.

### **4. Closing Procedures**

- The last person leaving a department must ensure all windows are closed and interior suite doors are locked.
- Ensure all high-value equipment (projectors, tablets) is stored in out-of-sight locations.

### **5. Incident Reporting**

- Report any suspicious individuals, unidentified packages, or unauthorized access attempts to [Name of Security Officer/Office Manager] at [Phone Number/Extension].

Compliance with these directives is mandatory. Failure to adhere to these security protocols may result in disciplinary action.

Signed,

[Signature]

[Printed Name and Title]