Oxford Policy Management

Physical Security Policy

08 June 2022

Definitions of Terms

Term	Definition
Board	The Board of Directors of OPM parent company
CIMT	Critical Incident Management Team: OPM's Management Team convened for incident response.
Contingency Plans	Plans devised for implementation following specific high impact risk events. OPM has three Contingency Plans: • Medical Evacuation • Hibernation and Relocation • Fire Safety
Duty of Care Centre	Online Risk Management data-feed for incident information – managed by Spearfish GSA.
Duty of Care	The legal obligation requiring standard of reasonable care by OPM in which people could be foreseeably harmed
Duty of Care Proforma	MS Excel tool for development of a security budget for use in all OPM client proposals
GSM	Global Security Manager: person responsible for security risk procedures in OPM
SSA	Senior Security Adviser: senior risk adviser to OPM, employed by our external security providers, Spearfish.
GSA	Global Security Analyst: manager responsible for Overwatch budgets and online information feeds, employed by our external security providers, Spearfish.
TA Form	Travel Approval Form: form to request approval for OPM representatives to travel to 'Medium', 'Low' and 'Negligible' risk destinations
HCRTA Form	High and Critical Risk Travel Approval Form: form to request approval for OPM representatives to travel to 'High' and 'Critical' risk destinations.
LHCRTA Form	Limited High and Critical Risk Travel Approval Form: for travellers to any destination working on a 'Fast Response' project
OPM	Oxford Policy Management Limited, all of its group and associated companies
Representative	Employees, Directors, sub-contractors, suppliers or anyone representing OPM over whom OPM has taken Duty of Care
Risk Rating	Designated risk rating for a specific destination as published within OPM's Risk Rating schedule on SharePoint – updated Quarterly.
PSR	Preventive Security Requirements: OPM's Framework for risk management.
PSR Scorecard	The agreed diary for implementation of the Project/International Office Security Plan.
Security SOP	Standard Operating Procedures for operational risk management – guides for travellers representing OPM.
SRA	Security Risk Analysis: context-specific risk analysis document prepared by GSM and Spearfish.

1 Introduction

This document sets out a framework for OPM's approach to dealing with the potential risks associated with Physical Security in our operational environments. It is designed to support our Representatives to reduce the impact and likelihood of risks encountered whilst working for OPM.

The Physical Security Policy is designed to ensure that OPM operates within appropriate Community Standards as outlined in the Duty of Care Statement, and to meet the seven Physical Security Directives of the *OPM Protective Security Requirements,* outlined below.

1.1 Scope

Risk exists in all contexts and so this Physical Security Policy exists to define OPM's responsibilities towards its Representatives and to provide operational guidance for those over whom it has Duty of Care.

All permanently established OPM entities are required to provide and maintain a safe working environment for their employees, contractors, clients and the public, and a secure physical environment for their official resources.

This policy does not form part of Staff contracts of employment. Notwithstanding, all Staff and Suppliers are subject to a general contractual obligation to comply with all relevant OPM policies including this policy, as amended from time to time.

1.2 Roles and Responsibilities

OPM's Chief Executive Officer ('**CEO**') is accountable to the Board for the safety and security of all OPM Representatives and has ultimate authority for security.

The Chief Operating Officer ('**COO**') has day to day authority and responsibility for all OPM Representatives.

The Global Security Manager (**'GSM'**) is responsible for managing the OPM Security Management System. Designated Country and Project Managers are responsible for implementing agreed Security Plans within their respective areas of operation.

All OPM Representatives have an individual responsibility to be aware of their safety and security obligations within the OPM Security Management System.

1.3 Physical Security Directives

Physical **Security** Policy Directives	
PHYSEC 1	OPM HQ Oxford must provide clear direction on physical security through the development and implementation of an operational physical security plan.
PHYSEC 2	OPM HQ Oxford must have in place policies and procedures to: • Identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific project locations. • Report incidents to management, human resources, security and law enforcement authorities, as appropriate

	• Provide information, training and counselling to employees • Maintain thorough records and statements on critical incidents
PHYSEC 3	OPM must ensure they fully integrate protective security early in the process of selecting, planning, designing and implementing projects.
PHYSEC 4	OPM must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.
PHYSEC 5	OPM must show a Duty of Care for the physical safety of those members of the public interacting directly with OPM.
PHYSEC 6	OPM must implement a level of physical security measures that minimises or removes the risk of information and information and communications technology (ICT) equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
PHYSEC 7	OPM must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. Donors, stakeholders and Partner Agencies may request OPM to implement heightened security levels.

2 Physical Security Policy and Planning

PHYSEC 1: The OPM Board and Senior Management Team must provide clear direction on physical security through the development and implementation of a Physical Security Policy, and address all physical security requirements as part of the OPM Security Plan.

The Policy is to:

- Detail the objectives, scope and approach to the management of physical security issues and risks within all OPM operations worldwide;
- Be endorsed by the Board;
- Identify physical security accountability and responsibilities;
- Explain the consequences for breaching the policy or circumventing any associated protective security measure; and
- Communicate on an on-going basis and be accessible to all OPM Representatives.

The Plan must:

- Continuously review physical security measures to reflect changes in the threat environment and take advantage of new cost-effective technologies; and
- Be consistent with the implementation of OPM's physical security risk analysis findings in each OPM operational area.

3 Protection of employees

PHYSEC 2: OPM is responsible for the health and safety of its representatives at work. This responsibility extends to situations where they are under threat of violence because of their duties or because of situations to which they are exposed.

OPM must have in place procedures to:

- Identify, protect and support its Representatives under threat of violence, based on a threat and risk assessment of specific operational areas or, where practicable, work locations;
- Report incidents to management, human resources, security and law enforcement authorities, as appropriate;
- Provide information, training and counselling to employees; and
- Maintain thorough records and statements on reported incidents.

4 New Bid Integration

PHYSEC 3: OPM must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying projects.

OPM are to:

- Provide information and access portals to facilitate appropriate security considerations for new client proposals;
- Demarcate a security management system for the selection, planning, design and implementation of project security based on threat and risk assessments;
- Include the necessary security specifications in planning, request for proposals and tender documentation, and
- Incorporate related costs in funding requirements.

5 Work Health and Safety

PHYSEC 4: OPM must ensure that any proposed physical security measure or activity does not breach relevant employer work health and safety obligations.

OPM are to:

- Conduct a risk assessment of any proposed physical security measure or activity and develop effective risk controls in line with a reasonably practicable approach; and
- Consider the likelihood and consequence of an accident or injury arising because of a physical security measure or activity and put in place appropriate control measures.

6 Duty of Care – third parties

PHYSEC 5: Where an OPM project involves providing services, OPM must ensure that Third Party personnel can transact with confidence about their physical wellbeing.

OPM are to:

- take all reasonable precautions which could avoid or reduce the risk of harm to Third Party personnel operating within our Duty of Care;
- choose the option which is least restrictive to the Third Party where there are options for several effective physical security measures which would reduce the risk of harm;
- ensure that OPM's physical security plan addresses the risk of harm to those Third Party personnel operating within OPM's Duty of Care; and
- develop relevant guidelines and procedures identifying the precautions to be taken to cover the identified risk factors.

7 **Physical security of ICT equipment and information**

PHYSEC 6: OPM must implement a level of physical security measures that minimizes or removes the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorization.

OPM are to:

- put in place appropriate building and entry control measures for areas used in the processing and storage of sensitive or confidential information;
- put in place physical security protection (which matches the assessed security risk of the aggregated information holdings) for all premises, storage facilities and cabling infrastructure;
- locate ICT equipment, where practical, in areas with access control measures in place to restrict use to authorized personnel only, and put in place other control methods where physical control measures are not possible;
- implement policies and processes to monitor and protect the use and/or maintenance of information, equipment, storage devices and media away from OPM premises, and in situations where a risk assessment determines, put in place additional control measures;
- implement policies and processes for the secure disposal and/or reuse of ICT equipment, storage devices and media (including delegation, approval, supervision, removal methods and training of employees) which match the assessed security risk of the information holdings stored on the asset, and
- implement general control policies which may include a clear desk and clear screen policy.

8 Physical security in emergency and increased threat situations

PHYSEC 7: OPM will develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. Donors, stakeholders and Partner Agencies may direct OPM to implement heightened security levels.

OPM are to:

- Co-ordinate physical security plans and procedures with other emergency prevention and response plans (e.g. fire, bomb threats, hazardous materials, power failures, evacuations, civil emergencies).
- Determine the approvals process for upgrade of risk ratings.
- Implement appropriate planning and training upgrades for affected project teams.
- Develop the capacity and competency to lead a Crisis Management response when deemed necessary, and
- Provide the contingent plans for escalation to a heightened level of risk.

Physical Security Policy

Document Purpose:

To reduce the risk exposure of those staff and suppliers over whom OPM has Duty of Care. This is done by providing a framework for OPM's approach to dealing with the potential risks associated with Physical Security in our operational environments.

Policy Overview			
Policy Owner	Global Security Manager		
Applies to	All staff and suppliers over whom OPM has Duty of Care		
Global or local scope	Global		
Version Number	3.0	**Effective from**	08/06/2022
Approvals (Dates)		**OPM Board**	08/06/2022
		Management Team	