Government Security

Industry Security Assurance Centre
A Government Security Centre

isac-group@mod.gov.uk

Industry Security Assurance Centre
Poplar-1 #2004
MOD Abbey Wood
Bristol BS34 8JH

IPSA Evidence Cover Sheet: Accreditation & Assurance

The form supports the submission of the information required for accreditation and assurance activities for Industry Personnel Security Assurance. Please provide the output as listed below for each of the 7 core elements of personnel security using the advice and guidance provided.

For any questions please contact the ISAC at the details provided above.

The SPF is available at the Cabinet Office website:
https://www.gov.uk/government/collections/government-security

A significant proportion of the GS007-Security is protected due to its sensitivity. These limited distribution documents are available via the ISAC. Details of this can be found on the DE&S PSyA website:
https://www.gov.uk/guidance/defence-equipment-and-support-principal-security-advisor

Company Details

ISAC Reference Number	Company Name

Section 1: Governance and Leadership

Positive and visible Board level support for protective security is vital to demonstrate to staff the value placed on personnel and people security policies and procedures.
Strong security leadership, at all levels across your organisation will:

- *Ensure consistency and clear lines of responsibility for the management of security risk*
- *Foster a multi-disciplinary approach to countering the insider threat*
- *Ensure proportionate and cost-effective use of resources*
- *Provide essential management information for the purposes of security planning and people management*
- *Provide a strong example that both develops and underpins an effective security culture.*

Area	Evidence Item	File Name	Page / Paragraph Number
PerSec Governance Framework	Organisation Charts		
	Governance and Leadership Processes		
Contract information	Contract tabs**	** IPSA Dashboard	
Comments (optional):			

Section 2: Insider Threat Risk Assessment

Understanding what Personnel Security (PerSec) risks your organisation faces is essential for developing the appropriate and proportionate security mitigation measures.

Area	Evidence Item	File Name	Page / Paragraph Number
PerSec Risk Management Framework	PerSec Risk Management Policy		
	PerSec Risk Management Processes		
	PerSec Risk Register Template		
	Insider Threat / PerSec Risk Review**	** IPSA Dashboard	

Comments (optional):

Section 3: Pre-Vetting Screening

Pre-vetting screening comprises the procedures involved in deciding an individual's suitability to hold NSV. This is not limited to new joiners, but also individuals already employed by an organisation who are moving into a role that requires NSV. All individuals must have been subject to BPSS checks and have a clear requirement to access classified material (Secret and above) prior to vetting sponsorship. This should include permanent, temporary and contract workers in the IPSA organisation and its network.

Area	Evidence Item	File Name	Page / Paragraph Number
Vetting Register	DART Accreditation for OS		
	Vetting Register Template		
	Clearance and network data**	** IPSA Dashboard	
Eligibility Considerations	Eligibility Policy		

Comments (optional):

Section 4: Ongoing Personnel Security

As per GS007 aftercare refers to the maintenance of effective ongoing personnel security management. Effective aftercare by NSV sponsors ensures that clearance-holders maintain the standards required to hold a clearance.

Area	Evidence Item	File Name	Page / Paragraph Number
Aftercare Framework	Aftercare Policy		
	Aftercare Processes		
	Aftercare data**	** IPSA Dashboard	
Comments (optional):			

Section 5: Monitoring & Assessment of Clearance-holders

Monitoring and assessment is an essential element of good personnel security. An holistic approach to protective monitoring is advocated, where information about Personnel Security risks are brought together under a single point of accountability and governance, to ensure a transparent, legal, ethical and proportionate protective monitoring capability. This includes conducting internal trend analysis activities to identify areas of vulnerability. This section is focused on the output of NSV clearance review activities.

Area	Evidence Item	File Name	Page / Paragraph Number
Clearance Review Protocols	Clearance Review Policy		
	Clearance Review Processes		
Behaviour Monitoring Protocols	Monitoring Policy		
Comments (optional):			

Section 6: Investigation and Disciplinary Practices

Many organisations will at some point need to carry out some kind of internal investigation into a member of staff. The primary duty for an investigator is to establish the true facts, whilst adhering to appropriate HR policy and employment laws.
With correct procedures in place employees who understand policies and regulations, and competent trained investigative staff, your organisation is better equipped to avoid these pitfalls and maintain trust.
In addition to investigating an insider act your organisation needs to have a risk management process in place which manages the consequences of the act and a process in place that helps you:

- *Identify and analyse the root cause of the incident;*
- *Identify the appropriate disciplinary actions or interventions that need to be undertaken;*
- *Assess the effectiveness of current control measures in place;*
- *Identify gaps in practice and;*
- *Develop more effective control measures.*

Area	Artefact	Artefact Name / File Title	Page / Paragraph Number
Incident Handling Framework	Incident Handling Policy		
	Incident Handling Processes		
	PerSec Incident Log output**	** IPSA Dashboard	
Disciplinary Framework	Disciplinary Policy		
	Disciplinary Processes		

Comments (optional):

Section7: Security Culture and Behavioural Change

A good security culture in your organisation is an essential component of a protective security regime and helps to mitigate against insider threats and external people threats (such as hostile reconnaissance).

Security culture is the set of values, shared by everyone in an organisation, which determine how people are expected to think about and approach security, and is essential to an effective personnel and people security regime.
The benefits of an effective security culture include:

- *employees are engaged with, and take responsibility for, security issues*
- *levels of compliance with protective security measures increase*
- *the risk of security incidents and breaches is reduced by encouraging employees to think and act in more security conscious ways*

employees are more likely to report behaviours/activities of concern

Area	Evidence Item	File Name	Page / Paragraph Number
Training Programme	PerSec Training Plan / Programme		
Communications Programme	PerSec Communication Plan / Programme		
Good Practice Repository	Good Practice Repository Description		

Comments (optional):

Additional Comments (optional):

Approved by:

Board Level Contact for <Client's Organisation>	Date	IPSA Assurance Team for ISAC	Date