SONY PICTURES ENTERTAINMENT

PRODUCTION SECURITY GUIDELINES (Tier 1)

Version 1.0
April 2024

SECURITY SAFETY & SUSTAINABILITY
PROTECTING OUR PEOPLE, PROPERTY & PLANET

TABLE OF CONTENTS

DOCUMENT HISTORY 2
TABLE OF CONTENTS 3
BEST PRACTICE OVERVIEW 4
Introduction 4
How to use this document 4
Risk assessment 4
Contacts 4
BEST PRACTICE GUIDELINES 5
1. Security risk management 6
2. Physical Security 8
3. Other protective security 11

OVERVIEW

Introduction

Sony Pictures Entertainment (SPE) is committed to providing a safe and secure work environment for our productions. SPE's Security, Safety and Sustainability (S3) team has developed these Production Security Guidelines to assist productions in achieving a high standard of physical security. The purpose of this document is to provide current and future production personnel and third-party vendors engaged by SPE productions with an understanding of general physical security expectations. In preparing these guidelines, SPE considered current industry best practices. Not all of the elements in this document will be applicable to all types of production activities. When implementing these guidelines, the production must also comply with any applicable local, state, regional and country laws or regulations

How to use this document

These Guidelines are a high-level, document, the contents of which will not be relevant to all types of production. Variables may include the scale, cost, location, and subject matter of the production. Productions are encouraged to review this document and determine which sections and/or subsections apply. Consideration should then be given to how each section/subsection can be implemented, where possible aiming to follow the implementation guidance. Productions might choose to delegate responsibly for implementation of specific parts to third-party vendors.

Risk assessment

A production's health, safety, security, and other risks should be identified through a comprehensive risk assessment, and appropriate control measures should be implemented to decrease risks to an acceptable level whilst ensuring that business objectives are met. Reviewing and implementing this guidance should run in parallel with, rather than replace, the production's risk assessment process.

Contacts

If you have any queries or comments about these guidelines, please contact your regional S3 representative.

SPE Global Security Operations Center (GSOC)

The GSOC is the communication focal point for SPE Security, Safety & Sustainability (S3) supporting business operations globally. The GSOC is manned 24 hours per day, 365 days per year, by a fully trained group of operators and analysts who can monitor and track all production locations and activity. Please ensure all security and safety incidents are reported to the GSOC in a timely manner. GSOC can be contacted as follows:

+1 310 244 5505/ GSOC@spe.sony.com

BEST PRACTICE GUIDELINES

The following guidelines provide a framework for assessing a production's ability to protect its people, assets, content and reputation. It is organised into three categories covering the following security topics:

1.	**Security risk management**	**2.**	**Physical security**	**3.**	**Other protective security**
1.	Security risk management	1.	Facility selection	1.	VIPs/talent
2.	Security organisation	2.	Perimeter security	2.	Crowds/audiences
3.	Communication	3.	Entry/exit points	3.	Travel security
4.	Policies and procedures	4.	Identification	4.	Personal security
5.	Training and awareness	5.	Visitors	5.	Emergency services
6.	Incident response	6.	Authorisation	6.	Firearms
7.	Business continuity and disaster recovery	7.	Electronic access control	7.	Threat intelligence
8.	Background checks	8.	Logging and monitoring		
9.	Confidentiality agreements	9.	Keys		
10.	Third-party use and screening	10.	Surveillance cameras		
11.	Security vendors	11.	Asset management		
12.	HoD Security or Security Coordinator	12.	Inventory tracking		
13.	Security culture	13.	Logistics (shipping)		
		14.	Logistics (receiving)		
		15.	Logistics (packaging)		
		16.	Transport vehicles		
		17.	Mail handling		
		18.	Barriers		
		19.	Hostile vehicle mitigation		
		20.	Drones		

1. Security risk management

Productions are advised to have a formal, documented security risk management process in place in order to identify and mitigate risks and vulnerabilities relevant to the production. Key elements of this are likely to be as follows:

1. **Security risk assessment**

   Develop a formal, documented security risk assessment process in order to identify risks and vulnerabilities relevant to the production.

2. **Security organisation**

   Identify security key points of contact and formally define roles and responsibilities.

3. **Communication**

   Establish clear lines of communication between the production, SPE and security vendors on security matters.

4. **Policies and procedures**

   Establish policies and procedures regarding security. Suggested topics to address include the following:

   a. Security incident reporting and management.
   b. Security and awareness training.
   c. Building and location security standards.
   d. Personal security.
   e. Photographs, filming, and recording.
   f. Acceptable use (e.g., social media, personal devices, mobile devices, etc.).
   g. Access control (including visitors) and identification.
   h. VIP/talent security.
   i. Contract guarding services.
   j. Mail handling.
   k. Equipment loss prevention.
   l. Asset and content classification and handling.
   m. Business continuity.
   n. Travel security (ideally as part of a wider travel risk management policy).

5. Productions are advised to communicate applicable security policies, procedures, and requirements to all production personnel (e.g., employees, temporary workers, interns) and third-party workers (e.g., contractors, freelancers, temp agencies). Keep records of the communication(s) and to whom distributed.

6. **Training and awareness**

   Develop (and keep up to date) a training and awareness program about security policies and procedures. Train production personnel and third-party workers upon hire and periodically thereafter.

7. **Incident response**

   Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team.

8. Business continuity and disaster recovery

Identify the business continuity team who will be responsible for detecting, analyzing, and remediating continuity incidents. Establish a formal plan that describes actions to be taken to ensure business continuity.

9. Background checks

To the extent legally permissible, consider whether background checks are appropriate for any specific positions, third parties or vendors. Review any proposed scope with the legal department.

10. Confidentiality agreements

Generally, most production personnel sign a confidentiality agreement (e.g., non-disclosure) upon hire. Review scope to determine if there are any gaps and consult with legal department to address as needed. Develop a process to ensure production personnel to return all content, assets, and client information in their possession upon termination of their employment or contract.

11. Third party use

Evaluate whether all third-party workers (e.g., freelancers) who handle content have signed confidentiality agreements (e.g., non-disclosure) upon engagement. Consult with legal department to address as needed. Develop a process to ensure all third-party workers to return all content and client information in their possession upon termination of their contract. Include security requirements in third-party contracts. Restrict third-party access to content/production areas and IT environments unless required for their job function.

12. Security vendors

Conduct due diligence with respect to all security vendors, including security guards, close protection, and security technology (CCTV, access control installation) companies. Ensure that all security vendors have their own Public Liability insurance. Ensure that security vendors employed by the production know and understand what performance is expected. Ensure that all security personnel have valid, in-date licenses to operate in whatever capacity they are employed. Ensure that all security vendors are fully briefed on their roles and responsibilities and that they understand the production's security standards and expectations.

13. HoD Security or Security Coordinator

For large-scale motion picture and TV production, consider appointing a Head of Department (HoD) for Security, or hire a Security Coordinator to act as de facto head of department for all security matters. The HoD Security or Security Coordinator's remit may include production security needs on-site (e.g., studio) and on location; physical/IP content protection; event security; executive/talent protection; and investigative support.

14. Security culture

Create a strong security culture in the following ways:

a. Soft measures:

- Lead by example. A good security culture relies on visible endorsement and engagement from the top.
- Develop clear and fit-for-purpose security policies (particularly on how to report security incidents) supported by training and regular communication.
- Ensure that staff are clear on how to report a security incident, and on their responsibilities in managing and resolving security risks.

b. Hard measures:

- Establish robust procedures for dealing with poor security behavior.
- Enforce security policies visibly and quickly when staff, contractors, or suppliers do not comply.

2. Physical Security

1. Facility selection

When selecting studios and other filming locations consider the existing physical security provisions in place at the site, in particular:

a. **Perimeter security**. Walls/fences/gates should span the entire perimeter of the site and be in a good state of repair; walls and fences should be 8 feet or higher.
b. **Vehicle entrance/exit point.** Should incorporate an electronic manned by security personnel, or an equivalent system, to control vehicle access into the facility.
c. **Security lighting**. Should ideally provide full coverage outside the facility to decrease risk of theft or security violations.
d. **External CCTV**. Sufficient external camera coverage around common exterior areas (e.g., parking, smoking areas).
e. **Alarms**. A centralised, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.). Effectively positioned motion detectors in restricted areas. Door prop alarms in restricted areas to notify when sensitive entry/exit points are open for longer than a pre-determined period of time.

2. Additional perimeter security

Implement perimeter security controls that address risks that the facility may be exposed to as identified by the production's risk assessment, based upon the location and layout of the facility, such as:

a. **Gates**. To be secured after hours.
b. **Signage.** Be cognizant of the overuse of production signage that could create targeting.
c. **Vehicle entrance/exit point.** Distribute parking permits to company personnel and third-party workers who have completed proper paperwork. Require visitor vehicles to present identification and ensure that all visitors have been pre-authorized to enter the premises.
d. **Security patrols**: Implement a daily security patrol process with a randomised schedule and document the patrol results in a log.

3. Entry/exit points

Always secure all entry/exit points of the facility, including loading dock doors and windows. Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas). Control access where there are co-located businesses in a facility.

4. Identification

For productions with 25 or more employees and third-party workers, provide personnel and long-term third-party workers (e.g., janitorial) with a photo identification badge that is required to be visible at all times.

5. Visitors

Develop a visitor access approval and tracking process. Elements to consider include, maintaining a visitors' log, issuing visitor identification badges**,** requiring visitors to be escorted by authorised employees while on-site, or

at the least in content/production areas, requiring a non-disclosure agreement (NDA).

6. Authorisation

Document and implement a process to manage facility access and keep records of any changes to access rights. Restrict access to production systems to authorised personnel only. Review access to restricted areas (e.g., vault, server/machine room) quarterly or when the roles or employment status of production personnel and/or third-party workers are changed.

7. Electronic access control

Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed. Restrict electronic access system administration to appropriate personnel. Store card stock and unassigned electronic access devices (e.g. keycards, key fobs) in a locked cabinet and ensure electronic access devices remain disabled prior to being assigned to personnel. Disable lost electronic access devices in the system before issuing a new electronic access device. Issue third-party access electronic access devices with a set expiration date.

8. Logging and monitoring

Log and regularly review electronic access to restricted areas for suspicious events. Report any suspicious electronic access activities that are detected to GSOC.

9. Keys

Limit the distribution of master keys and/or keys to restricted areas to authorised personnel only. Implement a check-in/check-out process to track and monitor the distribution of all keys to restricted areas. Use keys that can only be copied by a specific locksmith for exterior entry/exit points. Obtain all keys from terminated employees/third-parties or those who no longer need the access. Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.

10. Surveillance cameras

Where legally permissible and necessary, work with S3 to consider installing a surveillance camera system (analogue CCTV or IP cameras) that records all facility entry/exit points and restricted areas. Review camera positioning and recordings regularly to ensure adequate coverage, function, image quality, lighting conditions and frame rate. Restrict physical and/or remote access to the surveillance camera console and to camera equipment (e.g., DVRs, NVRs) to personnel responsible for administering/monitoring the system. Ensure that camera footage includes an accurate date and timestamp and develop an appropriate retain plan for camera surveillance footage and electronic access logs (e.g, for at least 90 days, or the maximum time allowed by law), in a secure location. Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately report detected security incidents to GSOC.

11. Asset management

Implement a classification scheme to categorise physical assets of differing security requirements. Establish an asset management system for digital and physical assets containing content or confidential information. Store high value assets (identified via the risk assessment process) in a restricted and secure area (e.g. vault, safe, or other secure storage location that is locked, access-controlled and monitored with surveillance cameras and/or security guards). Use studio film title aliases on physical assets and in asset tracking systems.

12. Inventory tracking

Develop a classification scheme to categorise physical assets of differing security requirements. Implement an asset management system to provide detailed tracking of physical assets, with a robust check-in/check-out process. Review logs from content asset management system regularly and research anomalies.

13. Logistics (shipping)

Track and log production asset shipping details. Validate client assets leaving the facility against a valid work/shipping order. Secure client assets that are waiting to be picked up. Prohibit couriers and delivery personnel from entering content/production areas of the facility. Document and maintain a record of all delivery personnel entering and exiting the building. Observe and monitor the on-site packing and sealing of trailers prior to shipping.

14. Logistics (receiving)

Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries. Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log). Perform the following actions immediately: tag (e.g., barcode, assign unique identifier) received assets; input the asset into the asset management system; move the asset to the restricted area (e.g., vault, safe).

15. Logistics (packaging)

Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages. Ship all client assets in closed/sealed containers and use locked containers depending on asset value. Implement at least one of the following controls: tamper-evident tape; tamper-evident packaging; tamper-evident seals (e.g., in the form of holograms); secure containers (e.g., Pelican case with a combination lock).

16. Transport vehicles

Ensure that all production vehicles are always parked in a secure location. Lock vehicles always, and do not place packages in clear view. Require security escorts to be used when delivering highly sensitive content to high-risk areas. Apply numbered seals on cargo doors for shipments of highly sensitive titles.

17. Mail handling

Establish and enforce a system for safe mail handling. See CPNI guidance at this LINK for reference.

18. Access Control

Access controls including barriers may be used for several reasons including to provide physical security, for example, to prevent production personnel and members of the public from getting close to a hazard. There are many different types of barriers. Any barrier/fencing used must be suitable for the purpose intended. The design must be capable of containing and protecting people, including small children. Note that raised concert-style 'pop barriers' can only be used if you have trained and experienced staff who are familiar with their operation and safety aspects.

19. Hostile vehicle mitigation

Vehicle-borne threats range from vandalism to sophisticated or aggressive attack by terrorists or determined criminals; consider hostile vehicle mitigation measures to counter these threats. Conduct a risk assessment to determine the threat and appropriate countermeasures. Mitigations may include: a robust system of vehicle identification for access to the site; an inspection procedure for parked vehicles; a traffic management plan for all areas of the site accessible by vehicles; vehicle security barriers to prevent access to certain areas (note: this is different to a standard vehicle barrier which may not stop a determined aggressor).

20. Unmanned aerial systems (UAS or 'drones')

UAS or drones can be used for numerous legitimate activities such as authorised filming and building inspections. However, they can also be used for purposes which present a security risk, such as unauthorised filming and hostile activities. Consider this in security risk assessments for both studio and location filming. Legislation and guidance concerning UAS varies in different countries; follow the advice of the relevant local civil aviation authority. Considering establishing a procedure for identifying and reporting UAS usage in the vicinity of a production.

3. Other protective security

1. VIPs/talent

Conduct a risk assessment to determine whether additional security measures may be necessary for those who may be considered VIPs or talent, for reasons of safeguarding them and others. Note: not all talent require close protection; this should be determined based on risk. Liaise with the SPE S3 team to determine the need for a specific security risk assessment, for example to help schedule their visit, to arrange additional security measures and if necessary, to liaise with the local police force to determine the need for their presence and/or support. Considering security, determine and control the level of publicity, marketing and communication which can be afforded.

2. Crowds/extras

Develop an entry access and identification system for crowds/extras. Verify the identity of all crowds/extras by requiring them to present valid photo identification (e.g., driver's license or government-issued ID). Make crowd/audience badges easily distinguishable from company personnel badges (e.g., colour coded plastic badges). Consider a daily rotation for paper badges or sticker colour. Consider using badges that change colour upon expiration. Log badge assignments upon entry/exit. Visitor badges should be sequentially numbered and tracked. Account for badges daily.

3. Travel security

Establish a travel security policy. Ideally this should be part of a wider travel risk management policy/program. Travel risk assessments should be produced for all travel undertaken by cast and crew when filming on location, including for tech recces/scouts. Travel risk assessment is necessary to ensure that all security, safety, and other risks have been identified and suitable control measures are in place. Travel risk assessment should include all forms of transport and accommodation to be used; general security threats; general threats to health. Produce travel risk management advice on a case-by-case basis. This may include country/location information; travel security advice; health advice; transport and accommodation considerations.

4. Personal security

Provide advice to cast and crew on taking precautions regarding their personal security, both in work time and away from it. This may include country/location information; travel security advice; health advice; transport and accommodation considerations.

5. Emergency services

When planning any medium to large scale location shoots, it is advisable to notify the police, fire, and ambulance services. The emergency services will need to ensure that your activities do not pose operational problems either at the scene or in the surrounding areas. Your regional S3 representative can facilitate liaison with the emergency services.

6. Firearms

SPE maintains a no firearms policy for any staff, visitors, or vendors while on an SPE property, affiliate campus, production set or special event.

7. Threat intelligence

Utilise threat intelligence platforms where available to inform the production of emerging potential threats to people, assets, content, or reputation. For instance, protests or public disorder in the immediate area. Utilise social media monitoring platforms where available to inform the production of emerging potential threats to people, assets, content, or reputation. For instance, fans intending to gain unauthorized access. SPE's Global Security Operations Centre (GSOC) can assist, via regional S3 representatives.

GUIDANCE ENDS.