POLICY & PROCEDURE

CONTROL ROOM OPERATOR & MONITORING CENTRE OPERATOR

The Purpose

To ensure all Techforce Security Staff employed in:

Control Room and Monitoring Centre Operations

 Deliver excellence in customer service and ensure the highest level of integrity, diligence and safety are strictly observed. Australian Legislation, Regulation and relevant Codes of Conduct are always at the forefront of any security operations role managed by TSS employees.

Note: All policies are subject to changes in legislation, which may supersede information outlined in this standard operating procedure.

NOTE: This document must be read in conjunction with Techforce Security Services Employee Handbook & Code of Conduct.

Policy

CONTROL ROOM MONITORING

Control Room Operations is regulated by a very defined Code of Practice which forms the basis of this Standard Operating Procedure:

• This Code of Practice contains the standards with which the Techforce Security Services will operate Control Room Operations Services.
• All Techforce Security Services staff associated with Control Room Operations must read and understand the code of practice.
• External agencies who have entered into Service Level Agreements with Techforce Security Services will act in accordance with the Service Level Agreements when dealing with the Control Room Operation.
• Access to the Control Room will be restricted to surveillance staff and other authorised personnel or visitors approved by the Client Manager or Organisation Representative.
• Staff employed to work in the Control Room, whether they are operators or managers, will meet the highest standards of probity.
OPERATIONAL INFORMATION

Ownership of the Control Rooms Operations

- The Client retains ownership of the Control Room systems and equipment, unless otherwise outlined in the Client Services Agreement.
- The Client has copyright of all, images, photographs and documentation in relation to the Control Room.

Operational Arrangements with Partner Agencies

- This Standard Operating Procedure will be supplemented by a set of policies, procedures and guidelines for the Control Room Operations.
- Involvement in any aspect of the Control Room system by any partner agencies or individuals will depend upon their willingness to comply with this Operating Procedure, any signed Service Level Agreements and policies and procedures set out by their respective organisations.

Determining Location and Design

Location

- When determining the placement of cameras, the client will assess to determine the priority of the installation in line with their own objectives.
- Techforce Security Services can act in a consulting capacity incorporating information on crime and safety offences. (As outlined in Adviser and Installer capacity).
- The cost of installing, maintaining and upgrading cameras and infrastructure and the capacity of the Control Room to monitor cameras is at the expense and responsibility of the Client.
- The location of the cameras will be clearly apparent to the public. This will be achieved with signage and information being made available on request and in line with the Client’s policies and procedures.

Design

- When adding additional cameras to the Control Room system, consideration needs to be given to current infrastructure and server capacity. In order to make the system more effective the cameras need to fit the activity occurring in the area.
- An assessment is carried out on any new location for Control Room cameras before any installation work is carried out. When the location has been approved the additional infrastructure is installed (if required).
- Once the infrastructure is in place the camera is installed and connected to the server via optic fibre and the images transmitted back to the Surveillance centre.
- Storage capacity is monitored to provide 31 days of recorded footage from each camera.
- Additional servers are added to the system when camera or recording capacity is reached.

CONTROL ROOM PURPOSE

- To reduce crime levels by deterring potential offenders;
- To reduce the fear of crime;
- To help ensure a fast, effective response in emergency situations;
- To assist in the detection and prosecution of offenders; and
- To help secure a safer environment for the client staff, customers and stakeholders.
- To monitor assets and property.
This policy also refers to any mobile or temporary cameras that may be installed for major or special events or other operation requirements.

RESPONSIBILITIES

Techforce Security Services will be responsible for the training and adherence of the Code of Practice for all staff and ensuring guard compliance with the principles contained within the Code.

Techforce Security Services will comply with the requirements for accountability set out in this Code of Practice and where necessary consult with and provide information to the public about the operation of the Control Room.

ACCOUNTABILITY

Techforce Security Services will carry out an annual audit of the Control Room which will include review of:

- Control room logs (visitor logs, electronic records, etc.);
- The content of recorded material;
- Applications for view/release of recorded material and
- Check of all equipment to ensure that it is in good working order.
- Any outstanding assessments of camera locations for future planning, functioning, management and operation of the system

The results of evaluation will be provided to the client as agreed and will form ongoing monitoring process as part of the Client Services Agreement.

PUBLIC INFORMATION

Clearly visible signs that cameras are operating will be displayed in the area covered by the cameras and at other key points. These signs will:

- Inform the public that cameras are in operation;
- Allow people entering the area to make a reasonable approximation of the area covered by the system; and
- Identify the client as the owner of the system.
- The Code of Practice will be available on request (subject to any other method outlined by the client);
- Enquiries in relation to the system and its operation are at the discretion of the Client.

MANAGEMENT OF CONTROL ROOM

Techforce Security Services has adopted:

- Effective and fair systems of recruitment and selection of staff which include measures to ensure that the selection process provides for thorough validation and suitability of candidates and regular reviews of the suitability of employed staff.
- A requirement that staff must be licensed, qualified at a suitable level on appointment and be capable of meeting in-service training requirements.
- A procedure which makes it plain that they risk disciplinary proceedings (including dismissal) if they breach any of the provisions of the Code of Conduct.
• A Procedure to ensure that access to the control room is restricted to operating staff and their managers and that the control room is protected from unauthorised access.
• A register detailing all instances of access to the Control Room CCTV facilities and associated property.

CONTROL AND OPERATION OF SURVEILLANCE EQUIPMENT

Use of the Control Room system
• All use of cameras will be in accordance with the standards of the Control Room Code of Practice, Protocols and Standard Operating Procedures.
• Cameras will not be used to look into adjacent or nearby premises or buildings, unless it is explicitly for the following (in real time) of participants in a crime, which originated in the public domain. Any misuse is to be treated as a breach of the Code of Practice and subject to disciplinary action.
• All Control Room staff will be made aware that recordings are subject to routine audit and they may be required to justify their interest in a particular member of the public or premises.
• Utilisation of the CCTV system by parties outside the Client Services Agreement requires prior approval from Client in writing.
• User access permitting viewing rights or operational use of the CCTV system can only be authorised by Client Managers or authorized personnel.

Additional Systems Equipment
Supplementation of the standard Control Room operation may be employed from time to time and can include (in consultation with the Client);
• Bollards for access control;
• Public address system to communicate with the public in view of the camera
• Licence Plate Recognition to monitor and locate vehicles moving through the Client premises or permit access to restricted areas
• Mobile camera towers to access areas on a temporary basis or areas that have no infrastructure.

RECORDED MATERIAL

Security of recorded material:
• Security measures will ensure that no unauthorised access to, alteration, disclosure, accidental loss or destruction of recorded material can occur.
• Recorded material will be treated according to defined procedures to ensure continuity of evidence.
• All recorded material will be subject to random inspection by either Techforce Security Services management team or Client representatives.

Access to recorded material:
• Partner Agencies, External Agencies or Individuals representing themselves in court for the purposes of legal proceedings, may make application to obtain footage from the Client;
• Partner Agencies or External Agencies are not permitted to remove any images or photograph, operate recording equipment or have contact with stored images or photograph at any time unless directed by the Client or subject to the execution of a search warrant or other relevant legal process.

Use of Recorded Material

• Recorded material will not be sold or used for commercial purposes or the provision of entertainment.
• The showing of recorded material to the public will be allowed in accordance with the needs of the Police in connection with the investigation of crime or in any other circumstances provided by law or as approved by the Client.
• Use of recorded material or photographs by the media will only occur with approval from the Client in accordance with their Media Handling/Corporate Affairs policy and procedures.

Applications for the viewing and/or supply of a recorded material (general):

• Access to and release of recorded material or photographs will only be permitted for reasons that are in accordance with the legal purposes or for reasons defined by the Client.

Footage will only be released to:

• Police - for the purpose of investigation or prosecution
• Client or Techforce Security Services Lawyers / Solicitors - for the purpose of legal defence of their client
• Any other parties must be determined by the Client.

Before any footage is released the following must occur:

• The correct paper work must be submitted and approved;
• Suitable identification is supplied that identifies the person collecting the footage

Release of original recorded materials

Original footage shall not leave the Control Room unless:

• it is delivered into the custody of the courts in response to a subpoena, search warrant, or other relevant legal process
• it is taken to court as evidence by a Control Room operator
• Or in other circumstances as determined by the Client and Techforce Security Services Management team.

Storage and destruction of recorded materials

• Recorded materials may be transferred to the Client arch archives in accordance with their Information Management Policy.
• All recorded materials returned to the Client will be either stored into the Archives or destroyed in accordance with the Clients Information Management Policy.
• Original recorded material and all copies of recorded material may be destroyed after 7 years from the date of application at the discretion of the Client.
Destruction of recorded materials shall be by burning, shredding, erasure or other approved method.

**BREACHES OF CODE**

Prime responsibility for ensuring the Code of Practice is adhered to rests with Techforce Security Services.

This responsibility includes ensuring that breaches of the Code are investigated and remedied to the extent that breaches of the Code are within the ambit of Techforce Security Services power to remedy.

**Resources**

- Standards in relation to the CCTV operation
- The CCTV Surveillance operations will conform to the Surveillance Device Act 1998
- The CCTV Surveillance operators and staff will abide by the Privacy Act 1988
- The CCTV System will follow the guidelines of the Western Australian Closed Circuit Television (CCTV) Guidelines

**Supporting Documentation (OPERATIONS MANUAL)**

- Control Room Access Log
- Control Room Equipment Register
- Control Room Equipment Maintenance Register
- Control Footage Access Register (Vic Pol & Legal only)