Devon & Cornwall Police

Force Policy & Procedure	**Protecting Information in STORM**
Reference Number	**D253**
Policy Version Date	**16 October 2018**
Review Date	**16 October 2021**
Policy Ownership:	**Alliance Operations Department**
Portfolio Holder:	**Assistant Chief Constable Local Policing & Connectivity**

Contents:

1. Policy Statement

1.1 This policy sets out the manner in which Devon and Cornwall Police will protect 'the need to know' in relation to sensitive information in the STORM Command and Control system. It reinforces the requirement of Incident Business Owners to ensure that appropriate control measures are in place to safeguard against inappropriate and unlawful access to Force systems. It also defines the criteria by which call-cards in STORM will attract enhanced security controls by way of 'view ratings'.

2. Introduction

2.1 The Force has a range of pre-existing measures to comply with the Government Security Classification (GSC) to control access to sensitive information, such as using access controls and lawful business monitoring. This policy sets out the **enhanced** protection measures to secure the 'need to know' principle. The STORM system allows for enhanced control measures to be applied to specific incident records, permitting access to identified groups of terminals, or individual members of staff, by the use of 'View Ratings'.

2.2 These controls form part of the STORM risk management accreditation document (RMADS) as required by the ACPO/ACPOS Community Security Policy (available via this link).

2.3 In the application of this policy staff are reminded of the need to comply with the standards and principles of the Code of Ethics for Policing.

3. Procedures

3.1 Procedures

3.1.1 It is envisaged that the Force's command and control system will only be used to record incidents that require operational command and control, therefore, access for staff will be for the purposes of their operational duty. The enhanced protection measures in STORM will only be implemented for specified individuals (or groups of) or terminals where the relevant criteria applies, and will only apply to a small number of incidents.

3.1.2 Access will be granted as required by role, and will be removed or amended if an individual with access leaves the force or moves into a role with no requirement for that level of system access.

3.1.3 Within the STORM system, the Force will apply 4 categories of view rating:

- **OFFICIAL Low incidents** – where no enhanced controls are required. The existing controls of access to STORM, password verification, existing business monitoring and compliance, provide the level of 'restriction' to information in line with GSC.

- **OFFICIAL Medium Incidents** – where view ratings will be applied to safeguard 'the need to know' in line with identified criteria.

- **OFFICIAL High Incidents** – where the highest level of control is required in the STORM system, providing access to the smallest number of pre-identified groups or individuals, and where a decision to use, or continue to use, STORM as the means of recording such information will need robust consideration.

- **ACIU** – Incidents with an ACIU view rating are accessible only by members of the Anti Corruption Intelligence Unit.

3.1.4 The Force Incident Manager (FIM) terminals will have access to incidents with OFFICIAL Medium and OFFICIAL High view ratings balancing the need to know with operational efficiency in applying such controls. The effective application of the 'need to know' principle requires those assigning enhanced controls to have operational responsibility for that information. This sits with the Force Incident Manager (FIM) and control room Sergeant.

3.1.5 Control room supervisor terminals will have access to OFFICIAL Medium incidents to allow for expediency in allowing RDOs access to these incidents where resourcing is a priority. The FIM or control room Sergeant may add control room supervisors to the OFFICIAL High view group when demand is high enough to impact the operational efficiency of either of these roles.

3.1.6 Where operational resources are required to have access to view an incident with a view rating, they will be attached to the incident in STORM, either by being 'informed' or 'dispatched' to the incident, which will grant them access to view that specific incident for the duration that they are attached to the log. This requires the resources to be correctly booked onto STORM.

3.1.7 Where control room staff require access to view rated incidents, terminals can be granted access to view OFFICIAL Medium or OFFICIAL High incidents. This is carried out on a 'need to know' basis and is at the discretion of the FIM or control room Sergeant based on the operational need to view the incident. These terminals will have the access removed once the operational requirement to view the incident is over.

3.1.8 Where owners of information require access to be controlled, careful consideration should be given as to whether STORM is the appropriate place to record it, and if so, the timing of the creation of that record – thereby minimising any risk of accidental or deliberate compromise.

3.1.9 When the command and control phases of an incident have been completed, consideration will be required as to the continued controls required on any record.

3.1.10 Built into STORM are automatic audit trails of actions taken to both control and open access to individual records; enabling compliance, audit, and lawful business monitoring.

3.1.11 Decisions by investigating officers in relation to legislative disclosure rules are separate to the judgements around enhanced controls in STORM.

3.2 Roles and Responsibilities

3.2.1 The duty FIM will initially be responsible for assessing the security requirements of an incident in line with this policy. Any other member of staff who considers that a view rating needs to be applied to any incident will bring the record to the attention of the FIM.

3.2.2 Predetermined access to specified individuals for OFFICAL Medium or OFFICIAL High incidents will be controlled to only the FIM and control room Sergeant.

3.2.3 Access on an incident-by-incident basis can be provided by the FIM or control room Sergeant upon identification of the 'need to know' principle. The FIM will assess the application of any view rating against the following criteria set out in the paragraphs below.

3.2.4 **OFFICIAL Low Incidents**
The vast majority of STORM records will not be assigned any form of view rating, and indeed to do so might adversely affect operational delivery.

3.2.5 **OFFICIAL Medium Incidents**
OFFICIAL Medium incidents are those where the compromise or misuse of the information poses a risk:

- Materially damage diplomatic relations
- Substantially damage national finances, economic or financial interests or viability of major organisations
- Seriously impede government policy
- Substantially disrupt national operations
- Substantially damage the operational effectiveness of the Force
- Substantially impede the investigation of a crime, or facilitate the commission of a serious crime
- Substantially prejudice individual liberty or security.

3.2.6 Examples would include: private visits by VIPs or members of the Royal Family, the initial stages of a serious or major crime intended to be managed in a covert manner (crimes in action, test purchase operations etc.), covert firearms operations, or incident records arising from sensitive intelligence sources (Operation Taurus).

3.2.7 Where an incident is being managed in an overt operational manner, it is unlikely that such restrictions will be necessary or have a clear practical benefit. Enhanced view ratings are used to protect incident records which attract one or more of the GSC categories. Incidents or complaints involving members of staff will only require a view rating where it relates to **sensitive information** (such as anti-corruption) that might cause 'substantial damage to operational effectiveness'.

3.2.8 During (the covert phase of) an operation such sensitivity may apply and the view rating should be removed when no longer necessary. For example, a 'sensitive view rating' applied during the planning stages of a search warrant or

public VIP visit should be removed when the operation moves to an overt stage (i.e. warrant is executed or public visit takes place). A view rating may still need to apply after the policing operation if the record holds intelligence or information that is still sensitive and not openly accessible through another source.

3.2.9 In order to safeguard the right to privacy of our staff, this level of enhanced security may be applied at the request of the appropriate Senior Management Team (SMT) member, or if dynamic, implemented by the FIM with a review by SMT at earliest opportunity.

3.2.10 **OFFICIAL High Incidents**
OFFICIAL High incidents are defined where compromise or misuse of the information poses a risk that could:

- Raise international tension
- Seriously damage relations for foreign governments
- Seriously damage the operational effectiveness of the UK Police Service
- Seriously damage the effectiveness of highly valuable security of intelligence assets or operations
- Cause serious damage to national finances, economic or financial interests or commercial interests
- Threaten life directly or seriously prejudice public order or individual security or liberty.

3.2.11 **Prior to the creation of an 'OFFICIAL High' view rating, careful consideration will be required as to whether the STORM system is, or remains, the appropriate method of recording such information. If necessary, the originator or FIM should liaise with the Force Intelligence Bureau (FIB) as to the other means available of achieving the operational objective.**

3.2.12 OFFICIAL High incidents provide the highest level of control in STORM. Providing access for the smallest number of pre-identified individuals and the protection (or continued protection) of an incident recorded in this way will require very careful consideration in order to balance the need to preserve the integrity and security, with the operational impact of limiting access to the incident record.

3.2.13 Examples might include: where 'secret' intelligence is contained within an incident log, an R v Osman operation, covert operations relating to major or serious crime, operations related to domestic extremism or terrorism, strategically sensitive covert firearms operations, or other operations involving sensitive military or other governmental/national assets.

4. Assessment Compliance

4.1 This policy has been drafted and audited to comply with the principles of the Human Rights Act. Equality and diversity issues have also been considered to ensure compliance with Equality legislation and policies. In addition Data Protection, Freedom of Information, Management of Police Information and Health and Safety issues have been considered. Adherence to this policy will therefore ensure compliance with all relevant legislations and internal policies.

5. Monitoring

5.1 Compliance with this policy will be monitored by:

- Incident reporting and escalation procedures
- Data protection audits
- Internal information security audits and inspections
- Independent audits

6. Review and Ownership

6.1 The review of the contents of this policy is the responsibility of the Commander Alliance Operations Department. Review of the policy will be undertaken annually.

7. Useful Links

7.1 Information Assurance Unit Intranet site

- D031 - Data Protection Policy
- D032 - Records Management Policy
- D091 - Force Physical Security Policy
- D313 - Information Sharing Policy
- D336 - Force Vetting Policy
- D338 - Lawful Business Monitoring Policy