Dunmow St Mary's Security Incidents Policy

A security incident is a confirmed breach, potential breach or 'near-miss' breach of one of ECC's information policies

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: If you discover a security incident, you must immediately **report** it
2. ***MUST***: When reporting the incident, you must **provide** as much information as possible
3. ***MUST***: The Data Controller must **complete** investigations as directed by the SIRO and complete an outcome report. See Procedures for Reporting or Handling a Security Incident.
4. ***MUST***: The Data Controller must support investigations as directed by the SIRO and provide an **outcome report**
5. ***MUST***: The Data Controller must oversee and support each investigation, maintaining a full **record** from reporting to closure
6. ***MUST***: The SIRO must support the investigation of **major and critical** incidents
7. ***MUST***: Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident

Why must I do it?

1. Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective
2. To help us quickly assess the severity of the incident and to speed up the investigation
3. Carry out an effective process appropriate to the severity of the incident
4. Carry out an effective process appropriate to the severity of the incident
5. Ensure the process is followed to completion
6. Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents
7. Ensure that all incidents are handled in a timely manner.

How must I do it?

1. Contact the data controller either by phone, email or face to face. If you would like to stay anonymous send a written letter/ report/note to the SBM, Data Controller. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible.
2. Include full details of the incident such as dates, names and any remedial action that has been taken.
3. Where appropriate, undertake the following:
    a. Identify expected outcomes, stakeholders and any policies breached.
    b. Speak to staff involved.
    c. Record evidence and keep an audit trail of events and evidence supporting decisions taken
    d. Get expert help
    e. Escalate
    f. Inform data subjects (service users, staff) where appropriate
    g. Identify and manage risks of the incident
    h. Commence disciplinary action, or record why not
    i. Develop and implement a communications plan where appropriate
    j. Put in place controls to prevent recurrence
    k. Complete the Incident Outcome Report
4. Where appropriate, undertake the following:
    a. Raise incidents through the Security Incident Management Procedure if reported to them
    b. Work with the DPO to investigate major security incidents.
    c. Decide whether to investigate personally, or allocate to the line manager/ investigating officer.
    d. Assess the outcome to ensure they are satisfied the appropriate action has been taken.
    e. Provide service area knowledge and advice, and to carry out any recommended actions within their function for major or critical incidents, where required.
5. Undertake the following:
    a. Classify the Security Incident
    b. Verify the details and oversee the investigation
    c. Work with the DPO to investigate major security incidents.
    d. Advise, support and intervene as appropriate
    e. Review Incident Outcome Reports and close

6. For major and critical incidents:
    a. Undertake the investigation (critical only)
    b. Work with DPO (major only)
    c. Assess if it is necessary for the security incident to be reported to the ICO.
    d. Complete an outcome report and recommend remedial actions.
7. Follow the process outlined in the ECC Procedures for Reporting or Handling a Security Incident

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Clare Griffiths, SIRO.

If you believe the policy does not meet your business needs, you may raise this with your Information Champion who, if they agree with your suggestion, may propose a policy change.

Document Control

Version: 1

Date approved: 24th April 2018

Approved by: Governing Body

Next review: 24th April 2021

References

- Data Protection 1968 (until 25th May 2018)
- General Data Protection Regulations 2016 (after 25th May 2018)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.