**Standard Operating Procedure**

**Information management**

| **Version:** 2, 08/04/2022**eDOCS:** 65236 |
| --- |

Contents

[1 Purpose 2](#_Toc100315122)

[2 Application/scope 2](#_Toc100315123)

[2.1 Process 2](#_Toc100315124)

[2.2 Principles 2](#_Toc100315125)

[3 Resources 3](#_Toc100315126)

[4 Warnings 3](#_Toc100315127)

[5 Abbreviations, acronyms and definitions 4](#_Toc100315128)

[6 Procedure 5](#_Toc100315129)

[6.1 Systems and resources 5](#_Toc100315130)

[6.1.1 eDOCS 5](#_Toc100315131)

[6.1.2 SharePoint 5](#_Toc100315132)

[6.1.3 BORIS 7](#_Toc100315133)

[6.1.4 Role based email accounts 9](#_Toc100315134)

[6.1.5 Microsoft (MS) Teams 9](#_Toc100315135)

[6.2 Large format displays of information 10](#_Toc100315136)

[6.3 Forms used in coordination and control centres 13](#_Toc100315137)

[7 Responsibilities and accountabilities 16](#_Toc100315138)

[8 Related and reference documents 16](#_Toc100315139)

[9 Appendices 16](#_Toc100315140)

|  |  |
| --- | --- |
| **Standard Operating Procedure (SOP)****Standard Operating Procedure****Information management**

| **Version:** 2, Date**eDOCS:** 65236 |
| --- |

 |
| Information management |

# Purpose

The purpose of this standard operating procedure (SOP) is to describe the actions and practices to be taken and systems to be used by personnel when planning and conducting information management within an incident or emergency response.

# Application/scope

This SOP is for all personnel involved in an incident or emergency response and describes the procedures that should be adopted and systems in place to ensure an efficient and effective response.

This SOP should be read in conjunction with Section 7 Information Management of the Biosecurity Emergency Operations Manual (BEOM).

## Process

Information is the basis of timely and appropriate decisions. The best use of information will follow a systematic handling of information.

The key steps are:

|  |  |
| --- | --- |
| * **Collection**
 | from multiple sources (history and real time) |
| * **Collation**
 | the sorting of information |
| * **Confirmation**
 | the verification of information collected and collated |
| * **Interpretation**
 | suitably skilled and authorised personnel make sense of information |
| * **Action**
 | response to the above actions |
| * **Distribution**
 | to appropriate parties |
| * **Storage**
 | in accordance with departmental policy and response requirements/obligations |

The actions are repeated constantly during a response and result in substantial quantities of information.

The sign of good information management is the capture, recording and filing of all information, to enable it to be retrieved and shared with as many interested and authorised personnel as possible – both during and post response.

## Principles

The fundamental principles of information management within a response are:

* Record as much as possible, either in writing or digitally (i.e. audio or film)
* Time and date everything
* Share information with all relevant parties in a timely manner
* All records are filed within eDOCS[[1]](#footnote-1) and other appropriate systems [[2]](#footnote-2),
* Actions are only to be taken by those who have the authority to do so.

When all these actions are executed well, the operation will “know what we know”. The information will not be lost, partially processed by a minority, or remain the knowledge of, or be visible to a single person/small group. As much relevant information as possible should be made available to as many personnel as is practicable.

All information generated during a response remains the property of the response. It is important to only use logs, forms and function specific notebooks (event logs) provided at coordination and control centres – do not use your own. When operating in a virtual control centre (VCC) environment all information must be digitised and registered in eDOCS.

# Resources

General –

* Access to the Incident and Emergency Responses file structure within eDOCS and the BEOM
* Access to the response specific file structure within eDOCS, SharePoint site and Microsoft Teams response Team site
* Access to response Biosecurity Online Resources and Information Systems (BORIS), as required
* Section manager arm bands
* General stationery
* Function specific notebooks for each position – no one is to use personal or work diaries etc.

Documentation

* Access to relevant documents available through the Document Management Guide (eDOCS: 21621) or BEOM SharePoint site for documents within eDOCS.

# Warnings

* Network/shared drives and applications such as Microsoft Teams and OneDrive are not deemed recordkeeping compliant and should not be used for the storage and management of records as they are unstructured and uncontrolled.
* Records should not be saved onto computer hard drives or USB sticks.
* Post Its should not be used as they can fall off documents and become lost or stick to other documents.

**Information Security and Privacy**

All response staff are responsible for protecting and respecting the personal information that we collect and hold, this includes any external provider or contractor that the department may engage, who will access or deal with personal information on behalf of the department (refer [Information privacy : DAF Intranet (resnet.qg)](https://dafintranet.lands.resnet.qg/information-knowledge/information-privacy) for more information).

Staff must also be aware of their security obligations and responsibilities, and adhere to the Information Security Management Policy, and associated security policy artefacts - Information Security Management Manual (refer [Information security : DAF Intranet (resnet.qg)](https://dafintranet.lands.resnet.qg/information-knowledge/security) for more information.

Response information and documentation must not be shared with personnel outside the response without authorisation from your section manager or the Coordinator/Controller.

Physical storage locations must be secured by lock and key to avoid loss or theft of hard copy documents.

The Records Management officer(s) should consider who requires access to physical and electronic locations as some sensitive information (e.g. positive laboratory test results or information about clients and properties) may need to be restricted.

**Right to Information (RTI)**

As biosecurity responses may be of significant interest to individuals and entities affected by the response, right to information requests relating to a response may be received. Applicants do not need to provide a reason for requesting information.

When working in a response environment (as with business-as-usual activities) staff should be mindful that documents and communications generated in the course of their duties can be subject to RTI requests. These can include texts, SMS and MS Teams chat messages, diaries, and diary notes (including personal diaries that contain work related information), computer files and other electronic data and emails (both work-related and personal).

**Human Rights**

Please note, when implementing this SOP you must consider whether any human rights are engaged under the *Human Rights Act 2019* and whether any limitations on human rights are reasonable and justifiable. If you engage a human right you should apply the procedure under the [Human Rights Policy](https://itpqld.sharepoint.com/sites/SPOBQ/Mixed%20business%20programs/Forms/AllItems.aspx?id=%2Fsites%2FSPOBQ%2FMixed%20business%20programs%2FPolicies%2FPolicy%20%2D%20Considering%20the%20Human%20Rights%20Act%202019%20in%20the%20application%20of%20policies%20and%20procedures%2Epdf&parent=%2Fsites%2FSPOBQ%2FMixed%20business%20programs%2FPolicies) and conduct a proportionality assessment under the Human Rights Act*.*

# Abbreviations, acronyms and definitions

| Term/acronym | Definition |
| --- | --- |
| BEOM | Biosecurity Emergency Operations Manual  |
| BORIS | Biosecurity Online Resources and Information Systems |
| eDOCS | Electronic document and records management system |
| FCP | Forward Command Post |
| IAP | Incident Action Plan |
| LCC | Local Control Centre |
| NFA | No further action |
| SCC | State Coordination Centre |
| VCC | Virtual Control Centre |
| WHS | Work Health and Safety |

# Procedure

## Systems and resources

Information management requires systems that enable the collection, collation, accessibility and exchange of information between coordination and control centres. This section outlines the systems and resources and how they are used during an emergency response to collect, manage, store and share information.

Before adding any additional applications, systems, technology or resources not listed within this document into the response, consider the records management requirements and if they can be met. If you are unsure, consult with the Records management officer.

### eDOCS

eDOCS is the Departments electronic document management system. It is the only system used in a biosecurity response that is records compliant; therefore, staff must ensure that all records (both electronic and hard copy) are stored and maintained in this system.

A generic and consistent eDOCS file structure template for emergency responses has been developed and approved ready for review and implementation by the Records management officer at the beginning of each response. The file structure template is based on the functions and activities described in AUSVETPLAN for all levels of a response i.e. SCC, LCC, FCP etc. and can be easily tailored to suit the size and type of response. It is recommended that response personnel familiarise themselves with the AUSVETPLAN functional structures, as this will assist greatly in navigation of response file structures during a response.

Shared network drives are not deemed recordkeeping compliant and are not to be used for the storage and management of records as they are unstructured, uncontrolled and are prone to complicating the operational necessity of having a single point of truth. Shared network drives should only be used for working documents (i.e. initial drafting) or as a temporary storage location (i.e. scanned hard copy documents). Emergency response records should also not be saved onto computer hard drives/desktops or USB memory sticks/flash drives.

### SharePoint

The response SharePoint site is considered the one point of truth and will be used to set the common operating picture of the response. This is most important where VCCs are in play as physical format displays won’t be in use when staff are working from home or a remote location. Sharing current up to date information with all response personnel in this virtual environment will be even more imperative.

This site is not to be used to create or house records. Records must first be saved in eDOCS and linked to the site. The site should also not be used to manage or share confidential or sensitive information.

During a response, permissions will be put in place that only allow read only access for most users. Access to the site will be managed through the Logistics section. The Records Management and Situation Assessment functions will be responsible for maintaining the site and ensuring all information and documentation is current.

The central tiles (refer to the section highlighted in red in figure 1) on the site, provide access to a number of key response systems and useful websites. Tiles can be added or removed to suit the requirements of the response. At a minimum the following tiles will be available following the establishment of the site:

* Case management (BORIS)
* Rosters (BORIS)
* Equipment (BORIS)
* BORIS people
* Public Information (BORIS)
* BQ Maps
* Bureau of Meteorology
* Biosecurity Emergency Operations Manual (BEOM)

The left-hand navigation pane (refer to the section highlighted in green in figure 1) on the site is where you will find all key documentation required to undertake operations within a response in a more user-friendly and easy to navigate environment. The format utilised to store key documentation, mirrors the functional file structure implemented in eDOCS for each individual response (refer figure 2 and 3).



**Figure 1 – Response SharePoint (Team Portal)**



**Figure 2 – Example of functional filing layout**



**Figure 3 – Example of how documents are displayed within the function**

### BORIS

BORIS is the main system used for collection, storage and retrieval of data generated in an incident or emergency response. Access to the required sites will be granted to personnel prior to deployment to a response.

BORIS comprises of several sites used specifically for incident or emergency responses. These include:

* Case management – Set up within the first 48 hours of a response, the site houses information specific to the pest/disease incursion and relevant cases such as property and customer data, surveillance data and observations, sample collection details and results, tracing data, destruction, disposal and decontamination activities, legislative tools and spatial (i.e. maps).

The case management site will mostly be used by the Coordination/Control, Planning and Operations functions.

Prior to the declaration of an emergency response i.e. during the investigation phase, personnel may record data in a pre-existing system such as Animal Health Surveillance, Plant Health Surveillance, Marine Pests, Animal Management etc. Once the emergency response has been declared and the pest/disease specific case management site established, the data from the pre-existing system may be transferred over to the new site – this will be requested through the Biosecurity Information Systems function, if required.

* Rosters – Managed by the Logistics section, Rosters delivers capability to generate rosters consistent with the organisational structure in AUSVETPLAN Control Centres Management Manual (Part 2).
* Equipment – Used by all staff in a response, the Equipment site allows users to electronically create, approve and action requests for equipment and to capture and manage information about assets and consumables that may be required for a response.

This site assists the logistics team with the allocation of assets assigned to a response. It is not an asset management system. Assets will still need to be managed in corporate systems such as SAP, as part of business as usual. If an asset is assigned to you, you are responsible for making sure that its record is kept updated as you will be expected to account for the whereabouts and condition of the asset. When you leave a response, it is your responsibility to ensure you reallocate the asset as part of the handover process.

* Public Information – This site allows staff within the Public Information section to capture information for activities undertaken and products developed as part of their function. Activities and products captured include advertising and publications, community and stakeholder engagement, internal communications, media including social media, e-Alerts and more.
* BORIS People – This site is designed to hold information about people who work on or may be asked to work on incident and emergency responses. All departmental employees, including contingent labour, are automatically listed in BORIS People. Third parties and external personnel can also be manually added to the site if and when required.

BORIS People is an information repository that holds data on peoples’ skills and training undertaken, response deployment history, licences held, allergies, immunisations and special dietary requirements. This information can assist the Logistics section to quickly identify people who have appropriate skills and training to undertake specific roles and/or have performed a similar role before. BORIS People also integrates with other parts of the BORIS platform, such as the rostering tool and the equipment module.

User guides for each BORIS site are available under the How To tab on each site.

BORIS Mobility – BORIS sites can also be set up to use an application (app) that can be accessed via iPads and/or iPhones to enable data capture in the field, even in areas out of mobile range. This app is known as BORIS Forms.

It is important to note that BORIS sites are not deemed records compliant, therefore documents should be loaded in eDOCS prior to being uploaded into BORIS. Any data entered into the system will need to be exported and captured in eDOCS.

### Role based email accounts

Role based email accounts (RBEAs) are a critical communication and information management tool which allow for a single email account to be used by several rostered personnel rotating through a designated position during the course of the response.

Personnel must only use their allocated RBEA during a response when corresponding by email. The use of RBEAs during a response does not negate the need for personnel to eDOCS emails that document business activities, decisions or transactions. Some key tips to keep in mind when dealing with emails in responses:

* Name email subject lines appropriately so that it is relevant to the purpose and content within.
* Rename the email subject lines where the subject of the content within the email changes - This makes searching for specific information/decisions/actions easier for new staff coming into a response or RTI requests after a response and allows the reader to quickly understand what action is required of them.
* All emails are to be saved within eDOCS especially those that document activities, decisions or transactions - Personnel may wish to wait until an email conversation is finished in order to capture the whole conversation as one record.
* Develop a system with the other account holders so emails are not overlooked or lost e.g.:
	+ Use a coloured flagging system to allocate tasks where more than one officer is utilising a RBEA.
	+ Turn the RBEA reading pane view off so that emails don’t show as having been ‘read’.
	+ If you read an email not meant for you make sure you re-mark it as unread so that the person it is intended for sees it. If you have implemented a coloured flagging system, flag the email for the person it is intended for.

### Microsoft (MS) Teams

A MS Teams site will be established at the beginning of each response and will be used as a tool for collaboration on documents, within a single section and across multiple sections and coordination/control centres.

Only one MS Teams site is to be created for each response. Additional Teams sites for the response are not to be requested or created unless absolutely necessary. If it is identified that there is a potential need for additional MS Teams sites a task request should be sent to the Logistics section for review and actioning, noting that consideration will need to be given to information management and shared situational awareness requirements.

The SCC Records Management function will create the file structure within this environment for personnel to work within when collaborating on documents. Personnel should not create their own folders. If additional folders are required, a task request should be sent to the Records Management function for consideration and action. The Records Management function will monitor these files regularly and unauthorised folders may be deleted.

MS Teams is not records compliant therefore all approvals, decisions or discussions within this environment are to be captured electronically and saved into eDOCS.

The response MS Teams site can also be used to host whole of response video briefings, if required. Meetings between smaller groups of response personnel should be set up outside of the response MS Teams site in this instance meeting requests should be sent to individuals business as usual email addresses not RBEAs. All meetings via MS Teams must have agendas, minutes, decisions and actions documented and captured in eDOCS.

## Large format displays of information

Information within Coordination/Control Centres should be displayed so that it is readily available to the relevant user and to all other personnel within the centre. These displays play a vital part in sharing as much information as possible with as many personnel as possible – “know what we know”. The SCC located on level 2, 41 George St, Brisbane has a number of electronic visual displays that can be utilised to help share information within the centre, refer to the State Coordination Centre SOP (eDOCS 6139894) for instructions on using these displays. In a VCC the response SharePoint site will become an even more important tool for sharing information and will replace the physical aspects of these displays.

All displays should be continuously updated and date/time annotated against entries or in the case of a graphic display, they should be marked “Correct as at *date/time*”.

All displays should be recorded either by photography or photocopy at strategic times e.g. mid shift, end of shift or at the end of an important phase or event.

Each of the following displays may be present in one or more sections as well as a central information or briefing area (in a VCC this would be the response SharePoint site).

Typical large format information displays include:

* **Event Board or Bulletin Board**
A Bulletin Board should be located at the entry to the Coordination/Control Centre, for information of response personnel and visitors. It should provide administrative information, summary of events and details of programmed events such as briefings, debriefings and press conferences. Information displayed may include an organisational outline complete with names of personnel filling positions, report schedules, the latest Sitreps or other briefings, media releases, roster shift changes, accommodation, transport schedules and other information relevant to relief personnel to enable updating prior to assuming duty. This board should also contain a map outlining important activities.
* **Futures Board**This board is one of the most important and the most overlooked boards in a Coordination/Control Centre. It should outline future events or problems so that they can be appropriately planned for and not forgotten. These boards should be in each section as well as one centrally located within the centre.
* **Key Contacts** (each section and Logistics)

This board should list contact details for key stakeholders in the operation. Contact phone and email address of organisations and personnel who are regularly contacted and used by more than one section in the Coordination or Control Centre should be permanently displayed.

The Logistics section should also ensure a contacts list of all response personnel is generated, maintained and made available to all personnel.

* **Major Events** (anything topical)

This is a running record of key events e.g. weather, Sitreps, injuries, media stories, listed as they happen.

* **Map Board(s)**These boards must be located with the Situation Board and Status Board to graphically display current information on appropriate maps of the operations areas. The maps should be marked with:
* The developing pest or disease/known information and intelligence from the field.
* Boundaries of the Restricted Area (RA) and Control Area (CA).
* Location of checkpoints on the boundaries of the RA.
* Location of all relevant properties e.g. Infected, Dangerous Contact and Suspect Premises.
* Routes designated for emergency response traffic movement/traffic control.
* Other relevant information as required.
1. **Notice boards** (Logistics Manager)

These should be strategically placed to provide timely information to all personnel. These boards should display media releases, any correspondence relevant to all personnel, and information such as rosters, accommodation, and catering arrangements.

A special board/space on a board may be set aside for “Special” notices/policy e.g. work health and safety (WHS) special notes.

1. **Operational area** (Operations, Planning)

Typically this is a map of the area, showing all operational activity, staging areas, etc.

1. **Operational deployment** (Operations, Planning, Logistics)

Shows which resource is deployed where, and at a point in time.

* **Resources Board**

A board is used to display resources already committed, as well as those available for deployment, including location, quantity, period applicable, duration, service requirements, estimated costs etc. of externally sourced resources. This information should be displayed near the Logistics Section. Some suggested headings are:

* Agency/functional area.
* Support/task.
* Location (where required).
* Number of personnel required/operational, etc.
* **Situation Board**
This board should be centrally located in the coordination/control centre and is used to summarise the current situation for the various locations affected by the incident/emergency. This board is to be constantly updated during operations, and forms the basis of information released to the public and media. Information that could be displayed includes:
* Numbers of premises within each status
* Destruction statistics – total number by species
* Compensation costs
* Resources deployed
* Staff deployed
* **Status Board**The status board should be centrally located within the coordination/control centre and summarises key information on all infected and dangerous contact premises**.**
* Case number and status (e.g. 3 DCP)
* Name
* Location
* Type of enterprise/property (e.g. cropping, grazing, feedlot)
* Host type (e.g. animal, plant/plant product, infrastructure etc.) and numbers
* Date legislative instrument invoked
* Stage of operations (e.g. valuation completed, destruction and disposal underway)
* Valuation estimate
* Source of contamination
* Comments
* **Team Dispatch Log**
Each Section Manager who has the responsibility of dispatching personnel should use a team dispatch log to be able to locate teams and to record the activities of assigned personnel. The boards should contain information on:
* Team members
* Location, premises to visit
* Tasks
* Mobile phone/radio call-sign
* Car rego
* Estimated time of return
* **Other Displays**Each Section should maintain any other display considered necessary. These will be relevant to the Section and may include:
* Property risk assessment
* Tracings
* Properties under surveillance, numbers waiting inspection/re-inspection
* Checkpoint locations and status
* Number of species counted, number destroyed, etc.

## Forms used in coordination and control centres

The processing of information relies initially on **collection, collation and interpretation**. Information is available from many sources – pre incident plans, history/records, field operations debriefings and Sitreps, government agencies such as the Bureau of Meteorology, and importantly local knowledge in its many forms.

A successful response depends on the timely capture of as much information as possible and sharing with as many interested parties as possible – in real time.

Only information of “value” needs to be recorded (i.e. information essential for the conduct of the response) so that it can be referred to and found and retrieved later. Post a response; it is essential a record, that traces activities/actions and decisions, be readily available. The same information is very useful during shift changeovers.

Forms are the basis of collecting, collating and sharing information. These forms also become key records and must be retained. Hyperlinked electronic forms are available through the Document Management Guide (eDOCS: 21621) for documents within eDOCS and the BEOM SharePoint site.

**Forms should be completed as you go** e.g. complete a Record of Conversation during the conversation.

Each completed form must show **a time and date** (when it is prepared), and legibly show the **author’s name**.

**All forms remain the property of the Coordination/Control Centre**. Only copies can be removed from the centre where authorised.

The following Forms should be in routine use during a response. Whilst other forms may be devised when required, the number of forms should be kept to a minimum.

1. **Communications Log**
	* This records the key details of each radio or telephone contact (time, unit, essence of the message).
	* Any messages requiring action e.g. field Sitrep, vehicle failure, injury, should have the information put into either a Message or Record of Conversation Form.
2. **Contact List**
* This lists the names/positions of key players (internal and external) and their contact details.
* It should be updated regularly – if necessary as it goes.
1. **Event Log (function specific notebook)**
* Every person within the response is required to maintain an operational log.
* The log is used as an immediate record of information received and actions taken.
* An event log may be in the form of a physical function specific notebook or electronic version (Refer to eDOCS: 21424)*.*
* Because logs could assume legal significance, it is wise to observe certain conventions in keeping them, such as:
* entries are made sequentially, and timed and dated
* every significant action is recorded
* entries are made as near as possible to the time of the event recorded
* no blank spaces or pages are left
* no pages are removed
* any alterations are signed and dated

All notebooks are to remain in the Coordination/Control Centre and are to be used by the next person on roster. When operating in a virtual control centre (VCC) environment these must be digitised, registered in eDOCS and forwarded to the incumbent as part of the handover process.

1. **Fax Log**
	* This records the key details of each fax transmission
	* A separate log should be kept for incoming and outgoing faxes in all but a small response
	* Refer to eDOCS: 21465 and 36563
	* All Incoming faxes are registered into the fax log sheet
	* This should be located beside the fax machine
	* To be managed by the Records Management officer who retains the original document
	* All outgoing faxes must be logged by the sender of the document
	* If there is sufficient staff this task can be performed by Records Management officer
	* All outgoing faxes must be scanned and captured in eDOCS.
2. **Incident Action Plan**This standard form should be developed for each shift – and shared with as many as possible prior to each shift. This template can be found at eDOCS: 21569 and in the Reports and Plans SOP eDOCS: 14371.
3. **Message Form**Very similar in format to the Conversation format (and inter-changeable) the Message Form is typically used to **issue an instruction or convey thoughts/information** (usually the product of only one person – Conversation is at least two sided). Refer to eDOCS: 21396*.*

There is provision for **Action**.

1. **Record of Conversation**Used to capture the key points of **any conversation/discussions** – especially those that may/will **result in an action**, either in the immediate or distant future. Almost all phone calls should be recorded – including those where there is no contact (record call made but no answer, or person not in).
* Interactions with/or about identified premises should be recorded in the BORIS Case Management system
* All other interactions should be recorded in the Record of Conversation register on the response SharePoint site or where this is not accessible or information is confidential or sensitive in nature it can be recorded using eDOCS: 21403 and saved in eDOCS.
1. **Sitrep**The standard form should be completed as much as possible at pre-determined times, even if there is no change in the situation. This template is available at eDOCS: 21568 and through the SOP: Reports and Plans eDOCS: 14371*.*
2. **Task and Resource Request**When you want a **resource, service, or task**, this form (refer to eDOCS: 21413) should be completed. Any requests for equipment should be made through the BORIS equipment site. A key requirement of both of these is **Approval** (by the person with the appropriate authority). The person making the request can give some indication of the source/provider of the service, resource etc.

Requests are best completed by the person making them stating **“what is required (the outcome)”, rather than how it might be achieved** (order a hole in the ground at a given site and of a given size to be completed by a given time rather than ask for excavators and trucks).

A data base (e.g. Excel) listing Task Requests should be set up early, to record any requests not captured in BORIS Equipment.

For more information refer SOP Task and resource request procedure (eDOCS: 14593)

# Responsibilities and accountabilities

|  |  |
| --- | --- |
| SCC Records Management function | Is responsible for:* Establishing a central filing structure and defined storage locations
* Monitoring defined storage locations to ensure compliance
* Providing advice and assistance to the Situation Assessment function with maintaining the common operating picture (via SharePoint) for the response
 |
| Situation Assessment function | Is responsible for:* Maintaining a common operating picture in the form of the response SharePoint site with assistance and advice from the Records management function
 |
| Logistics section | Is responsible for:* Providing response staff with access to systems required to undertake their duties
* Maintaining and sharing current response organisational structure and key contact lists of all response staff
 |
| Section managers/Heads of functions | Are responsible for: * Ensuring all personnel within their section are trained in information management systems and comply with information management processes.
 |

# Related and reference documents

|  |  |
| --- | --- |
| Form | Event Log (eDOCS: 21424) |
|  | Fax Log (eDOCS 21465 and 36563) |
|  | Record of conversation (eDOCS 21403) |
|  | Task resource request (eDOCS 21413) |
| Framework | QGEA strategic framework |
| Guide | Document management guide (eDOCS: 21621) |
| Manual | Biosecurity Emergency Operations Manual (eDOCS: 33397) – Sections 7 and 10 |
| Standard Operating Procedure | Records Management function (eDOCS: 5160813) |
|  | Creating and managing role based email accounts (eDOCS: 3316443) |
|  | State Coordination Centre (eDOCS 6139894) |
|  | Reports and plans (eDOCS 14371) |
|  | Task and resource request procedure (eDOCS 14593) |
| Template | Incident action plan (eDOCS 21569) |
|  | Situation report (eDOCS 21568) |

# Appendices

Nil

**Control page**

|  |  |  |
| --- | --- | --- |
| **Author/s** | Name: | Lisa Hickey |
| Title: | Senior Project Officer, Biosecurity Emergency Operations |
| **Reviewing officer/s** | Name: |  |
| **Approved by** | Name: | Stacey Hook |
| Title: | Manager, Biosecurity Emergency Operations |

|  |  |
| --- | --- |
| **Issue/approval date** | 08/04/2022 |

**Revision history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Issue Date** | **Amendment details** | **Editor/s** | **Approved by** |
| 1 | 02/11/2011 | First issue | David Learoyd, Kevin Cooper, Glen Akers, Debbie Rainbird, Debbie Beetson, Kevin Duff | Rob Johnson |
| 2 | 08/04/2022 | Full review and update with current practices. Update to new template.  | Lisa Hickey | Stacey Hook |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

eDOCS reference number 65236

**Review and amendments**

This SOP will be reviewed every two years and a revision issued as necessary. Suggestions and recommendations for amendments should be forwarded to:

Attention:

The Manager, Biosecurity Emergency Operations

Biosecurity Queensland

Department of Agriculture and Fisheries

Email: stacey.hook@daf.qld.gov.au

1. An incident and emergency response file structure will be established within eDOCS and will be available during a response [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)