Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Information management in emergency operations

Effective information management contributes to the resolution of the emergency by:

- supporting decision making, planning, reporting and monitoring of progress
- supporting communication of the situation to emergency personnel and other stakeholders
- preserving an accurate record of operational activities, including evidence for auditing, investigation and assessment purposes
- aiding compliance to legislation and standards

Incident related information remains the property of the NSW Department of Primary Industries (DPI).

Roles and responsibilities

Response personnel:

- record and store data accurately with time, date, name and role (if not part of system metadata)
- maintain confidentiality to protect the people impacted by the emergency and to minimise the risk of inadvertent, inappropriate and/or unauthorised use
- must not share or display information system login details and must report security breaches immediately

Planning function:

- ensure the effective and efficient management of information with specific responsibilities in the DPI Planning and Intelligence emergency response roles
- may include the rostering of personnel to manage hard copy information

State Emergency Coordinator:

- requests activation and deactivation of systems (see Appendix 4)
- approve system configuration, upgrades and changes during a response

Systems, Intelligence and Traceability (SIT) Unit:

- activates and deactivates information systems (see Appendix 4), including the archive of records at the end of the incident, as requested by State Emergency Coordinator

CSP portal

- address system failures and technical issues

Logistics

- provide the following at induction and during shifts
    - internet log in access, including Wi-Fi passwords
    - supply electronic devices (by task requests)

Resources

- Refer to guide Set up of control centres
- Government agency personnel may be requested to bring compatible portable electronic devices, such as laptops, mobile phones, tablets, radios and satellite phones, to use during a response (where that will not inconvenience work colleagues)
- Electronic devices, such as laptops, mobile phones, tablets, radios and satellite phones, will be issued by Logistics where required
- Access to internet provides access to response resource documents, community information and assorted technical information (particularly for biosecurity responses)
- Access to systems (i.e. generic, organisational and emergency management).Restrictions to the type and level of information may apply and usually relates to assigned emergency response role

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Managing information

Information is collected across the entire response from many sources by a variety of means, stored, analysed and disseminated to support the safe resolution of the emergency. Key systems are listed below. Information should be collected and stored in the primary information system (designated to manage the specific data) to ensure accessibility, e.g. task requests in WebEOC.

Alternate options of managing information are required in the event telecommunication and/or electricity is unavailable.

1. Google Drive

Google Drive stores, shares and manages documents in a generic folder structure (Appendix 1) created for each control centre; requires personnel to:

a. store information in the appropriate folder
b. access master copy of forms (see below) from the EM Resources or Google Drive and complete by hand or electronically
c. ensure filenames accurately describe the content and include the date (and time when relevant) – date format 'yymmdd' will result in sequential listings in date order
d. save files as another file with a different date for each day's edit or as required e.g. Accommodation register LCC Dubbo 180430
e. sub-folders (to the generic folder structure) can be tailored to the response
f. scan hard copy documents, store in appropriate folder
g. only share documents and folders with relevant response role accounts (not personnel accounts) unless approved by the State Coordination Centre
h. policies, procedures, forms and supporting documents are managed according to procedure Control of emergency management documents
i. not save data to computer or external hard drives

2. Email

Emergency response email accounts collect, store and disseminate information. Each role has a designated email account, assigned at induction. Some roles will have shared email accounts. Rules of use include:

a. use response email account, not your normal business accounts to allow for a single point of contact
b. enter the role/s or person/s who are to action the email in 'To' field; roles/people who are being provided information are in the 'CC' field
c. complete the 'subject' field with a meaningful description of the email content
d. email 'signature' to include your name, role, control centre location, and role contact phone number
e. move actioned/completed emails from the inbox into folders (which have labels similar to the Google folder structure in Appendix 1)

3. Forms

Forms apply when data is not collected directly into an online system or when online systems are inaccessible. Forms are located at EM Resources and publications. Copies can be made and used in the appropriate incident Google Drive folder or as a hard copy.

Forms completed routinely by response personnel include:

a. Event log – daily record of actions, conversations and decisions for each role. Event log book remains with the role; time and date for all entries
b. Record of conversation – conversations that will result in action e.g. safety issues, complaints, enquiry from the community
c. Sign-on register – to log entry/exit to a site and attendance at induction

Forms completed in Planning function to disseminate information

a. Incident Action Plan (IAP) – details mission and objectives providing direction to resolve the emergency
b. Situation report (sitrep) – report on response progress and any issues compiled, approved and distributed to key stakeholders at regular intervals (i.e. usually daily). File names must include the Incident name and version of the sitrep.

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

4. Hard copy filing

Hard copy filing system is maintained by Planning to ensure maximum sharing of information and retention of key records. Key points are:

a. Originals should be centrally filed as they are created, with copies distributed if required
b. Additions on copies require it to be filed with the original
c. Files borrowed from the central file must be logged
d. Each function in the control centre must have clearly labelled in/out trays which are regularly cleared
e. Filing system labels should be consistent with Google Drive folder structure (in Appendix 1)
f. Originals of legal documents (i.e. contain a signature) must be filed and archived after the incident. Examples include contracts, biosecurity directions and permits. Refer to the policy Records management.

5. Apps

Apps are software programs for a specific purpose. A list of recommended Apps for phones, tablets and computers are listed in Appendix 2; additional apps may be required in the response.

6. Images

Photos and videos are a visual record. Refer to guide Photos and videos in emergency operations.

7. EMtrain

EMtrain is a training management system which collects and stores training records. Personnel are required to complete online induction (prior to start of first shift) and response specific training. Access is according to the user guide.

8. WebEOC

WebEOC is a resource management system to collect, store and display information including task requests, personnel records (e.g. contact details, qualifications), personnel availability, rosters and photo identification cards.

a. Refer to user manuals for access instructions and business rules. Note: system access (i.e. user name and password) will not change between normal business and response
b. WebEOC training is available in EMtrain and varies with response roles
c. Response roles will be assigned to personnel in WebEOC allowing access to incident data

9. BioMAP

BioMAP is a mapping system integrated with core Biosecurity and Food Safety information systems

a. Access is requested via the CSP portal prior to a response or will be supplied at induction for the relevant roles
b. Training is available only via the department intranet

10. Biosecurity Information System (BIS)

BIS is the case management system and is used to record all property and case related activities

a. Access is requested via the CSP portal prior to a response or will be supplied at induction for the relevant roles
b. Training will be provided as part of your response role induction and training

11. Organisational (department) systems

Access is generally restricted to NSW Department of Industry personnel, using normal login details. Access and training is available through department processes. Refer to the department's intranet for details.

Organisational systems are relevant in emergencies:

For all personnel

1. Incident notification reporting and investigation – report all safety incidents
2. CSP portal for technology, finance and human resource support
   a. Process emergency management worksheets
   b. Address system access and failures logged by Communications Support response role
3. Records management in CM9
   a. Limited to state level outward documents

4. Purchase card reconciliation system e.g. Expense8
   a. All purchase card transactions in a response must be approved in a task request by an emergency response role with emergency financial delegation

Logistics/Finance personnel

5. Finance and human resources management system
6. Travel management system

Restricted access

7. Laboratory records in SampleManager

12. Status boards

Status boards are large format displays (e.g. electronic displays, notice boards, whiteboards) in the control centre/evacuation site to keep response personnel and the community informed

   a. information included will vary with the response type and location and purpose of the board; suggestions in Appendix 3
   b. contains 'correct at time/date'
   c. confidentiality of affected people must be maintained

Safety

Safety issues must be addressed by implementing appropriate controls. Risks may include:

- Fatigue management
- Manual handling

Further information

Department of Industry policies

- Records management policy (IND-I-177)

DPI emergency management information

- DPI emergency management resources and publications (includes original forms/templates)
- DPI current response situation
- Information to assist the community with emergencies

Other agencies

- Office of Emergency Management
- NSW Rural Fire Service
- NSW State Emergency Services

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Appendices

Appendix 1 – Google Drive folder structure

Google Drive folders	Details of content
Incident name	
• State/Local [insert name of LLC]/FCP [insert name of FCP]	Structure applies to all levels of the incident. LLC and FCP need to be differentiated with locations e.g. LLC – Dubbo or FCP – Dunedoo.
• Control	
o Safety	
o Industry Liaison	
o Agency Liaison	
o Monitoring and audits	
• Finance	
o Accounts	Storage of financial receipts (temporary), contracts
o Financial reporting & monitoring	Storage of financial reports
o Compensation	*Biosecurity responses only*
• Logistics	
o Accommodation	All accommodation information including provider register and room allocations
o Catering	All catering information including suppliers list and dietary requirements reports
o Communications support	All communications coordination including asset assignment (phones, tablets, radios, communications hub) and networking details
o Facilities	All facilities related coordination including security, access conditions, contracts (if not in finance), cleaning and services
o Personnel	Storage of contracts (if not in finance) and personnel information not recorded in WebEOC, including timesheets
o Travel and motor vehicles	All travel details coordinated on behalf of responders including flights, hire cars, pool vehicles and any other ground support vehicle
o Medical Services	Records of provision of medical support such as first aid kits/rooms/services
• Operations - Biosecurity	*Only loaded for Biosecurity responses*
o Infected Premises Operations	Should include folders for Inventory, Valuation, Destruction, Disposal, Decontamination, Pest Animal Control
o Movements	Should include folders for Permits, Mobile Security, Directions
o Investigations – surveillance	
o Investigations - tracing	
o Vaccination	
o Resource management	Tracking of resources, e.g. equipment register
• Operations – Natural disaster/Locusts	*Only loaded for natural disasters and locusts responses.*
o Surveillance - aerial	Includes damage assessments
o Surveillance - ground	Includes damage assessments
o Destruction and disposal	
o Animal welfare and treatment	Includes water and fodder assessments and deliveries

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Google Drive folders	Details of content
o Evacuation sites	Animal registers
o Resource management	Tracking of resources, e.g. equipment register
• Planning/Intelligence	
o Documents	According to the procedure Control of EM documents
▪ Approved	
▪ Archived	
▪ Draft	
▪ Final unapproved	
o Photos and videos	All incident photos and videos to be recorded and labelled according to the guide Photos and video in emergency operations
o Plans	IAP and supporting plans, eg medical, communications, resources, community engagement. *Sub-folders may include draft, final unapproved, approved and archived – similar to documents (above).*
o Situation & analysis	Situation report and supporting information
o Registry	Event logs, briefings, debriefings
▪ Event Logs	Folder per function
▪ Briefings / debriefings	Folder per function
▪ Records of conversation	Folder per function
o Resources	Records to track resources including equipment, consumables and suppliers registers e.g. PPE register
o Communication	Details to support communications planning unit
o Technical advice/liaison	
o Mapping	Mapping information and supporting information
• Public Information	
o Media	Media messages, interview management information
o Community Liaison	Public meeting notes, organisation of meetings
o Information and warnings	Storage of fliers, generic information (eg disease fact sheets)

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Appendix 2 – Apps for (mobile) devices

Apps are software programs (on a mobile device or a computer) designed to perform a specific function.

Recommended apps will be installed on response devices and may be useful for normal work activities. Check the iTunes App store or Google Play for more information including reviews on current versions.

Agencies and organisations

Fires near me NSW

Floods near me NSW

IFAW Wildlife Rescue

WIRES Wildlife Rescue

ABS statistics

NSW RealTime Water Data

Water Live

RFS PocketBook

Safety

Live Traffic NSW

First Aid

Find my friends

Find my iPhone

Emergency+

Weather

Australian Bureau of Meteorology

Weatherzone

Tides near me

Google and recording data

Google drive

Google Earth

Google maps

Voice recorder

PDF scanner

News

ABC News

Nine Network News

7 News

SBS News

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Appendix 3 – Status boards

Information can be displayed in electronic or hard copy format.

Electronic information can be configured as a dashboard and/or have rotating screens of information.

Personnel must be assigned to ensure information is kept current.

Types of information (listed in the table below) can be on stand-alone boards or combined.

Planning function is responsible for implementing and maintaining most status boards in a control centre. Other functions may use them for their specific information (as noted in 'Information' in table below).

Information	Details / examples
Mission and objectives	Incident name, mission and objectives Stand alone and part of IAP Situation reports
Maps (printed or electronic displays)	Area of operation: • Flood – extent of inundation with flood levels • Fire – fire scars • Biosecurity – properties by case status Operational area with sectors, staging areas, resource distribution
Daily schedule	Schedule of key meetings, e.g. IMT, state, national or cross border
Threat	Disease/pest manual, fact sheets Predictions of threat movement (see IAP)
Weather	Forecast e.g. Bureau of Meteorology satellite images, weather warnings
Organisational chart	Key roles and people currently in the roles, e.g. IMT
Communication	Diagram of communication network Lists of key contacts – may vary based on location of information e.g. operations and logistics lists will be different
Resources (personnel)	Data or map includes numbers of personnel by skill/role, location, status Roster displayed
Resources (physical)	Data or map of numbers of key equipment by location, status
Operational totals *(Operations function)*	Natural disasters – Request for assistance status, animal numbers by status Biosecurity – numbers for surveillance, tracing, destruction, disposal, decontamination, permits etc
Task status *(Planning/Logistics/Operations functions)*	List of current task request status
Media (television, print, Apps) *(Public Information function)*	News – television news programs, papers Social media feeds
Issues/notices *(Control/Planning/Logistics functions)*	Safety risks – medical plans, evacuation plans Operational risks Reminders to staff
Messages board *(all functions)*	Location to leave messages for personnel
General notice board for response personnel – combine information above *(Planning/Logistics functions)*	May include media releases, sitreps, IAPs, new operational policies/procedures, rosters, accommodation, catering arrangements, safety notices, well-being support contacts
General notice board for community *(Public Information/Planning/Logistics functions)*	Contacts for financial/well-being support, community meeting locations/date/time, details of available services, safety notices, current situation

Emergency Management Unit
Biosecurity and Food Safety
Email: emergency.preparedness@dpi.nsw.gov.au

Appendix 4 – Activation and deactivating information management systems

Activating information systems

Information systems are implemented at the commencement of emergency operations. Systems are activated within one hour of a request from the State Emergency Coordinator or delegate to the SIT Unit.

Activation for emergency management (EM) and generic systems includes:

- creating an incident in WebEOC and assigning initial role access
- providing logistics with WebEOC Position Access Codes and associated details
- activating the case management system
- issue of mobile device for field data capture
- contacting BTS with a list of emergency response roles for activation of email addresses and Google Drive
- implementing a Google folder structure within Google Drive (similar to Appendix 1) and providing access to all roles activated for the response as per notification to BTS
- providing appropriate BioMAP access for first responders.

Response personnel may have access to some systems prior to the emergency incident. Accessing information systems remains the same i.e login and password details will not change. As part of the emergency operations, personnel will be given access to the incident information which may vary with their response role.

Department (organisational) systems remain the responsibility of the Department of Industry. Access (i.e. login and password details) and responsibilities of users will not change in an emergency.

Once systems are activated they become the responsibility of the response personnel to manage including the assignment of personnel to roles within the systems. Any issues are escalated to the appropriate department unit, usually by the Communications Support role in the response structure.

Deactivating information systems

Information captured during a response must remain available for interrogation and reporting after the conclusion of the response in accordance with the Department of Industry policy for Record management. All information related to the response is to be archived, including information stored in BIS, BioMAP, WebEOC, emails and Google Drive.

Archiving requires:

1. State Emergency Coordinator to request incident information to be archived after the incident has concluded and all records are considered complete.
2. SIT Unit to archive information and provide details to the State Emergency Coordinator regarding methods of access for interrogation and reporting.

Deactivating information systems may also require:

1. removing access to incident records
2. archiving remaining hard copies (including originals of legal documents) in the department's record management system.