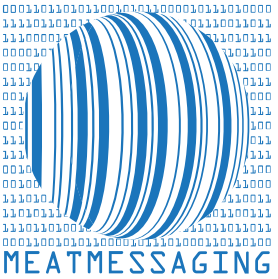


# Meat Messaging

- **Cyber Security Policy**
- **Information Systems Security Practices**

**Prepared by: Des Bowler**
**Issue date: 30th September 2021**
**Version: 1.01**
**Review date: 30th September 2022**

# 1. Contents

# 2. Cyber Security Policy Purpose and Scope

## 2.1 Policy Purpose

Meat Messaging's cyber security policy outlines the principles and processes that ensure confidentiality, integrity and availability of information by providing protection against malicious and accidental threats. This policy enforces a frame work to manage Cyber security risks and threats that take advantage of weaknesses in technology, people and processes to harm information. Meat Messaging manages cyber security risk to safeguard its core objectives as an Australian meat industry traceability portal and to protect the interests of the organisations those information it holds.

This policy establishes Meat Messaging's cyber security risk management and responsibilities, and is based on the principle that cyber security is everyone's business. Management of cyber security risk requires a concerted effort across all operational activities related to Meat Messaging and cannot be considered just an aspect of information technology.

## 2.2 Policy Scope

This policy is broad and applies to parties that interact with the Meat Messaging meat industry traceability portal, including:

- Meat Messaging personnel;
- Registered 3rd parties that upload data to Meat Messaging meat industry traceability portal;
- Non-registered 3rd parties that access the Meat Messaging meat industry traceability portal and the Meat Messaging App.

## 2.3 Policy Authority

Meat Messaging is administered by AUS-MEAT with program management through a steering committee (RMSCC) comprising of industry representatives including AUS-MEAT, DAWE, AMPC, AMIC and MLA. This policy has the authority of the Meat Messaging steering committee.

# 3. Security Practices and Requirements

## 3.1 Context

This section of the document outlines the security practices and requirements that are to be followed by those parties defined in the scope of this documents.

## 3.2 Information Security Management

The mitigate risk and protect data held within the Meat Messaging meat industry traceability portal against increasingly aggressive and sophisticated cyber threats.

The mitigate steps include:

1. All users and organisations (including Meat Messaging operational personnel) that are registered to use Meat Messaging have reviewed and accepted the terms and conditions of use include the responsibilities of use.
2. Periodically revalidating the users and organisation that are registered to use Meat Messaging including revalidating the acceptance of the terms and condition of use.
3. The functions to add, modify or delete data are controlled through processes that require authorisation and unique identification of the authenticated entity.
4. Transaction logs are created of all access to and actions related to adding, modifying or deleting data within the Meat Messaging Systems. These logs identified the unique identification of the authenticated entity.
5. The Meat Messaging meat industry traceability portal located and maintained of platforms that have a known locations and ensuring the known location of all data storage.
6. The Meat Messaging meat industry traceability portal located and maintained of platforms that have physical and virtual (cyber) security protocols that meet current industry security protocols and the security protocols requirements of industry and government.
7. The accuracy and commercial suitability of the information placed in to the Meat Messaging meat industry traceability portal is the responsibility of the organisations that places the information.

## 3.3 Cyber Security Risk Management

Cyber security controls seek to reduce cyber security risk by either reducing the likelihood or impact of an incident, or both. Meat Messaging actively seeks to identify and treat cyber security risk via the following measures:

1. Operating processes for identification and actioning of abnormal activities related to Meat Messaging.
2. Monitoring Meat Messaging platforms for cyber security vulnerabilities and taking rapid action to address any identified the vulnerabilities.
3. Ensuring the all patches and updates to environments and applications are completed in a timely manner.
4. Ensuring all Meat Messaging operational personnel are familiar and follow this and related policies, practices and requirements.
5. Conduct internal audits on the operational and monitoring processing and functions to ensure compliance to this and related policies, practices and requirements.

## 3.4 Recording and Reporting

Meat Messaging producers a range reports that are provided to the Meat Messaging steering committee against the reporting scheduled. The reporting areas include:

1. System usage,
2. User base,
3. Message volumes,
4. Cyber security metrics,
5. Security related Incidents, including data spills or other breaches.