GRAIN TRADE AUSTRALIA
Grain Trade Australia Limited
PO Box R1829 Royal Exchange NSW 1225
Phone: +61 2 9235 2155 Fax: +61 2 9235 0194
Email: admin@graintrade.org.au Web: www.graintrade.org.au

GTA Information Technology Advisory Committee

Technical Guideline Document (TGD)

Cyber Security in the Australian Grain Industry

1. Introduction

This Technical Guideline Document (TGD) refers to industry minimum practice for managing cyber security risks across the Australian grain supply chain.

This TGD complements the Australian Grain Industry Code of Practice (GTA Code of Practice) and other relevant industry and regulatory frameworks (as may be amended from time to time), including guidance issued by the Australian Cyber Security Centre and internationally recognised standards.

The information contained in this TGD is provided as general guidance on cyber security risk management only. Given the evolving nature of cyber threats, technologies, and regulatory requirements, there may be delays, omissions, or inaccuracies in information contained in this document.

This document outlines:

- The nature of cyber security risks within the grain industry
- Industry obligations in managing those risks
- Recommended practices and controls
- Actions to be undertaken in the event of a cyber incident

2. Discussion on Cyber Security Risks

2.1 What is a Cyber Security Risk

In the context of this TGD, a cyber security risk is any risk associated with the use, operation, or reliance on information technology (IT), operational technology (OT), or digital systems that may result in:

- Disruption to any supply chain activity including grain receival, storage, handling, transport and processing
- Loss, corruption, or unauthorised access to data
- Financial loss, including fraud or contractual impacts
- Breaches of regulatory or contractual obligations
- Safety risks arising from compromised operational systems

Cyber security risks may arise from:

- Malicious activity (e.g. ransomware, phishing, unauthorised access); or
- Non-malicious events (e.g. system failure, human error, configuration issues).

2.2 Cyber Risk in the Australian Grain Industry

The Australian grain industry operates within a complex, interconnected supply chain that is increasingly dependent on digital systems.

Key characteristics include:

- Use of casual labour during peak periods, shared bulk handling infrastructure, transport assets and processing facilities
- Reliance on operational technology (OT) such as weighbridges, Program Logic Controls and automation controls
- Integration of commodity trading, logistics, and financial systems
- Dependence on third-party service providers, including transport, storage, and administration and technology vendors
- Operation across regional and remote environments, which may present additional cyber security challenges

Cyber incidents may have heightened impact during critical operational periods, including:

- Harvest periods, where system availability is essential for receival operations
- Heavy domestic and export periods, where delays may result in contractual and financial consequences

2.3 Causes of Cyber Security Incidents

Cyber security incidents may arise from a range of causes, including but not limited to:

- Phishing or social engineering attacks targeting personnel
- Weak or compromised user credentials
- Unpatched or vulnerable systems
- Inadequate segregation between IT and OT systems
- Unauthorised access by internal or external parties
- Compromise of third-party systems or services
- Inadequate monitoring or detection capabilities

2.4 How Cyber Incidents are Detected

Cyber incidents may be detected through several means, including:

a) Internal Detection

- System alerts or monitoring tools identifying unusual activity
- Staff reporting suspicious emails, system behaviour, or unauthorised access
- Detection of anomalies in operational data (e.g. weighbridge or quality data inconsistencies)

b) External Detection

- Notification from third-party service providers or vendors
- Advice from customers, counterparties, or financial institutions
- Alerts or advisories issued by government agencies or regulators

3. Obligations on Industry

As outlined in the GTA Code of Practice, industry participants are expected to:

- Manage risks associated with the storage, handling, and movement of grain, including cyber-related risks
- Maintain the integrity, accuracy, and reliability of data associated with grain transactions
- Ensure systems supporting commercial and operational activities are fit for purpose and appropriately secured

- Take appropriate action where incidents occur that may impact the supply chain

Where a cyber incident results in potential breaches of contractual or regulatory obligations, industry participants are expected to:

- Investigate the cause of the incident
- Implement appropriate remedial actions
- Communicate with relevant stakeholders where required

Failure to comply with these obligations may result in:

- Financial loss to individual participants
- Contractual disputes
- Loss of market access or customer confidence
- Broader impacts to the reputation of the Australian grain industry

4. Recommended Cyber Security Practices

Industry participants should implement cyber security controls appropriate to their size, complexity, and risk profile. The following practices are recommended as a minimum baseline.

4.1 Governance and Risk Management

- Cyber security risks should be incorporated into organisational risk management frameworks
- Roles and responsibilities for cyber security should be clearly defined
- Policies and procedures should be documented and periodically reviewed

4.2 Access Control

- Multi-factor authentication should be implemented for critical systems
- Access to systems should be limited based on business need (least privilege principle)
- User access should be reviewed periodically and revoked when no longer required

4.3 IT System Security

- Systems should be maintained with current security patches and updates
- Endpoint protection measures should be implemented
- Systems should be securely configured, with unnecessary services disabled

4.4 Operational Technology (OT) Security

Given the importance of OT systems within the grain supply chain:

- Access to OT systems (e.g. weighbridges, conveyors, automation systems) should be restricted
- OT networks should be segregated from corporate IT networks where practicable
- Changes to operational data should be monitored and controlled
- Backup and recovery processes for OT systems should be maintained

4.5 Data Protection

- Sensitive data (e.g. contracts, pricing, customer information) should be identified and protected
- Data should be backed up regularly, with backups tested for recoverability
- Data shared with third parties should be appropriately secured

4.6 Third-Party Risk Management

- Cyber security risks associated with third-party providers should be assessed
- Contracts should include appropriate cyber security expectations where relevant
- Third-party access to systems should be controlled and monitored

4.7 Incident Response

- An incident response plan should be documented and maintained
- Roles and responsibilities during an incident should be clearly defined
- Incident response processes should be tested periodically

4.8 Business Continuity

- Critical business functions should be identified
- Contingency arrangements should be established to maintain operations during system outages
- Business continuity plans should consider cyber incident scenarios

4.9 Awareness and Training

- Personnel should receive regular cyber security awareness training
- Training should address risks such as phishing and payment fraud
- Seasonal and casual staff should be included where relevant

4.10 Monitoring and Detection

- Systems should generate logs of key activities
- Monitoring processes should be implemented to detect suspicious activity
- Alerts should be investigated in a timely manner

5. Actions to Undertake Following a Cyber Incident

Responses to cyber incidents will vary depending on the nature and severity of the incident. The following actions should be considered where relevant.

5.1 Confirming the Incident

- Validate that an incident has occurred
- Determine the scope and impact of the incident
- Identify affected systems, data, and operations

5.2 Containment and Response

- Isolate affected systems to prevent further impact
- Implement temporary controls where required
- Engage internal or external technical support

5.3 Communication and Reporting

- Notify relevant internal stakeholders
- Communicate with customers, counterparties, or regulators where required
- Consider reporting to relevant authorities where applicable

5.4 Remedial and Follow-Up Actions

Following resolution of the incident, actions may include:

- Restoring systems and data from backups
- Identifying root cause and implementing corrective actions
- Reviewing third-party involvement
- Enhancing controls to reduce likelihood of recurrence
- Reviewing training and awareness requirements

6. Harvest Readiness

Given the increased risk during harvest, industry participants should undertake pre-season preparedness activities.

Recommended actions include:

- Ensuring systems are patched and up to date
- Verifying that backups are functional and recoverable
- Reviewing and updating incident response plans
- Confirming staff awareness and training
- Reviewing third-party access arrangements
- Validating contingency processes, including manual workarounds

---

7. Further Information

Industry participants may refer to the following resources:

- Australian Cyber Security Centre – Essential Eight
- National Institute of Standards and Technology Cybersecurity Framework
- ISO/IEC 27001

---

8. Disclaimer

This TGD provides general guidance only and does not replace individual organisational risk assessments, contractual obligations, or applicable laws and regulations.

---

9. Review of this Document

This TGD should be reviewed periodically to ensure it remains current with industry practices, emerging threats, and regulatory developments.

- **Committee to discuss**

End: