

# Trans Dragon Cyber Security Policy

## 1. Purpose

Trans Dragon is committed to protecting its information assets, ensuring the confidentiality, integrity, and availability of data, and mitigating cyber risks. This policy outlines the framework for managing cybersecurity across the organization, aligned with the 10 privacy principles.

## 2. Scope

This policy applies to all employees, contractors, and third parties who access Trans Dragon's systems, networks, or data.

## 3. Cyber Security Principles and Procedures

### 3.1 Risk Management

- Conduct regular risk assessments to identify and evaluate threats to information assets.
- Prioritize risks based on impact and likelihood, and implement appropriate controls.
- Review and update risk management strategies annually or as needed.

### 3.2 Secure Configuration

- Ensure all systems, databases, and software are configured securely and updated promptly.
- Disable or remove unnecessary functionalities to minimize vulnerabilities.
- Apply patches and security updates in a timely manner.

### 3.3 Home and Mobile Working

- Implement secure remote access solutions (e.g., VPNs, multi-factor authentication).
- Enforce policies for protecting company-issued devices (laptops, mobile phones) and removable media.
- Require encryption for sensitive data accessed or stored remotely.

### 3.4 Incident Management

- Establish a documented incident response plan to address security breaches.
- Conduct regular backups and test restoration procedures to ensure business continuity.
- Assign roles and responsibilities for incident handling and reporting.

### 3.5 Malware Prevention

- Deploy and maintain anti-malware software on all company devices.
- Restrict unauthorized software installations and enforce email/web filtering.
- Train employees to recognize and report phishing and other malicious activities.

### 3.6 Managing User Access

- Implement role-based access controls (RBAC) to limit access to sensitive systems.
- Conduct periodic access reviews to ensure permissions align with job roles.
- Enforce strong password policies and multi-factor authentication (MFA) where applicable.

### 3.7 Monitoring

- Monitor networks and systems for suspicious activity using intrusion detection/prevention systems (IDS/IPS).
- Log and analyze security events to detect and respond to incidents promptly.
- Retain logs for a defined period to support investigations.

### 3.8 Network Security

- Secure network perimeters with firewalls and segment networks to limit lateral movement.
- Encrypt sensitive data in transit (e.g., TLS for web traffic).
- Regularly audit network configurations for vulnerabilities.

### 3.9 Removable Media Controls

- Restrict the use of removable media (USB drives, external hard disks) to authorized personnel.
- Encrypt all data stored on removable devices.
- Implement policies for reporting lost or stolen media.

### 3.10 Accountability, User Education, and Awareness

- Provide mandatory cybersecurity training for all employees during annual induction update.
- Provide online training to include phishing simulations and security awareness campaigns.
- Foster a culture of security by encouraging employees to report suspicious activities.

#### **4. Roles and Responsibilities**

- Mr H Duan – IT & Facilities Manager: Implement and maintain security controls, monitor systems, and respond to incidents.
- Scott Willis – Director of International Services: Allocate resources, enforce compliance, and support cybersecurity initiatives.
- All Trans Dragon Employees: Adhere to security policies, report incidents, and participate in training.

#### **5. Compliance and Enforcement**

- Non-compliance with this policy may result in disciplinary action.
- Regular audits will be conducted by the IT & Facilities Manager to ensure adherence to cybersecurity measures.

#### **6. Policy Review**

This policy will be reviewed annually or as needed to address emerging threats and regulatory changes.

#### **Approved by:**

Mr H Duan

IT & Facilities Manager

Trans Dragon International

April 22<sup>nd</sup> 2025