

# CAST COMMERCIAL ACUMEN LIMITED

## Data Leakage Controls

The following protocols are used to minimise and prevent data leakage at Cast Commercial Acumen Limited (“the Company”).

### 1. Identification of Sensitive Data

To prevent data leakage, we begin by identifying our sensitive data and its location within the Company. Then, we identify which information requires the highest levels of protection and categorise the data accordingly.

Once our most sensitive data has been identified, we then take the most appropriate security measures, which will include access controls, encryption, and data loss prevention (DLP) software. It may also be appropriate storing such sensitive data in the cloud.

### 2. Evaluate Third-Party Risk

Third-party risk is the threat presented to organisations from outside parties that provide services or products and access privileged systems. This risk is significant because third parties do not necessarily have the same protection and security standards as our organisation, and we will have no influence on or control over their security practices.

Here are two ways we will monitor and assess the risk of third parties:

- i. Where possible and appropriate, evaluate the data security attitude and policies of all vendors to ensure that they are not likely to experience a data breach.
- ii. Conduct vendor risk assessments to ensure third-party compliance with regulatory standards, such as GDPR, PCI-DSS, and voluntary standards like SOC-2.

### 3. Secret Management & Protection

Secrets management refers to tools and methods for managing digital authentication credentials (Secrets), including passwords, keys, API’s, tokens for use in applications, IT services, privileged accounts, and other sensitive parts of our IT ecosystem.

Secrets Management is important because passwords and keys are some of the most commonly used and important tools we have for authenticating applications and users and providing them with access to sensitive systems, services, and information. Because secrets have to be transmitted securely, secrets management must account for and mitigate the risks to these secrets, both in transit and at rest.

As a small company we need to ensure vigilance to protect against our potential vulnerabilities by:

- i. **Using dual factor authentication.**

- ii. **Enforcing password security best practices** including password length, complexity, uniqueness, expiration, rotation across all types of passwords. If a secret is shared it should be changed immediately.
- iii. **Extend secrets management to third parties** to understand their policies, practices and confirm agreement to our best practices.

As we grow as an organisation, we can start to incorporate the following suggested best practices:

- i. **Discover / identify all types of passwords** and bring them under centralised management system.
- ii. **Eliminate hardcoded and embedded secrets** helps us to remove dangerous backdoors into our IT ecosystem.
- iii. **Rigorous security parameters** to more sensitive tools and systems, e.g., one-time passwords and rotation after use.
- iv. **Apply privileged session monitoring** for accounts users, automation tools to improve oversight and accountability.

#### 4. Secure all Endpoints.

An endpoint is a remote access point that communicates with an organisational IT network autonomously or via end-users. Endpoints include computers, mobile devices, and Internet devices.

Like most organisations the Company adopts some remote working model. Consequently, our endpoints are geographically dispersed, making them difficult to control and secure.

Whilst our VPNs and firewalls provide a base layer of endpoint security, these measures are not always sufficient. Malware can trick our employees into permitting attackers to enter our IT ecosystem, bypassing these security measures.

As a small business we aim to prevent endpoint related threats through educating our employees to identify cyber attacker tricks, specifically those used for social engineering and email phishing attacks.

As we grow, we will invest in modern endpoint protection technology which can provide multi-layered protection for our organisational IT endpoints.

#### 5. Data Encryption

Encryption is the conversion of data from readable information to an encoded format. Encrypted data can only be processed or read once you have decrypted it.

Where appropriate, the Company will use data encryption to make it difficult for cybercriminals to exploit any potential data leaks.

## 6. Evaluate Permissions

We need to be constantly vigilant about who has access to our most sensitive data, and ask the question ‘do actually need and require access?’

The Company regularly evaluates permissions to ensure we don’t give access to unauthorised parties.


The Company categorises data into different levels of sensitivity to control access to the different pools of information. Only trusted employees who need and require access will have permissions to what is considered highly sensitive information.

The Company has a policy of regularly reviewing privileges to ensure permissions and access to sensitive data is only granted to those who need it.

## 7. Protocol Review and Implementation

7.1. These protocols will be updated as necessary to reflect the size of the Company, current best practice, official guidance, and in line with current legislation.

7.2. These protocols shall be deemed effective as of 13th April 2023.

<b>Document title:</b>	Data Leakage Controls
<b>Document status:</b>	Final
<b>Version number:</b>	1.0
<b>Date:</b>	April 2023
<b>Review date:</b>	April 2025
<b>Owner:</b>	Managing Director
<b>Approved by:</b>	Clayton John Ainger
<b>Signature:</b>	

**These Data Leakage Controls are not contractual and may be varied by Cast Commercial Acumen Limited at any time.**