

# Endorsement

## Gold Complete

**Endorsement Number**

**This endorsement, effective**

**Issued to**

Issued by the **Insurer** and applicable to the following Section(s) only:

### **Absolute Privacy Event and Security Failure Exclusion**

---

In consideration of the premium, the policy is amended as follows:

#### **ABSOLUTE PRIVACY EVENT AND SECURITY FAILURE EXCLUSION**

1. The following exclusion is added to the General Policy Exclusions Section of the Policy:

The **Insurer** shall not be liable under this Policy to make any payment for **Loss** or any other amount of any **Insured Entity** or **Corporate Superannuation Trustee** arising out of, based upon, or attributable to or in connection with any actual or alleged **Privacy Event** or **Security Failure**.

2. The following exclusion is added to the Crime Protection Section and applies to all Extensions in that Policy Section:

The **Insurer** shall not be liable to make any payment:

- (i) of any **Defence Costs**, fees, costs, expenses or charges; or
- (ii) pursuant to the "Erroneous Funds Transfer" Extension or the "Consequential Penalties" Extension,

arising out of based upon, or attributable to, or in connection with any actual or alleged **Privacy Event** or **Security Failure**.

The following definitions apply to this endorsement:

### **Breach of Confidential Information**

the loss or unauthorised access to, modification, disclosure or transmission of **Confidential Information**.

### **Company Computer System**

- (i) any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the Internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by an **Insured Entity** or **Corporate Superannuation Trustee**;
- (ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system;
- (iii) any employee "Bring Your Own Device" used to access any of the foregoing computer hardware, software or components thereof or **Data** contained therein; and
- (iv) any cloud service or other hosted computer resources, used by an **Insured Entity** or **Corporate Superannuation Trustee** and operated by a **Third Party** service provider under a written contract between such **Third Party** service provider and an **Insured Entity** or **Corporate Superannuation Trustee**.

### **Confidential Information**

**Corporate Information** and **Personal Information** in an **Insured Entity's**, **Corporate Superannuation Trustee's** or **Information Holder's** care, custody or control or for which an **Insured Entity** or **Corporate Superannuation Trustee** is legally responsible.

### **Corporate Information**

a **Third Party's** items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

### **Data**

any electronically stored digital or digitised information or media. For the purposes of this endorsement, **Data** is not tangible property.

### **Data Protection Legislation**

the *Privacy Act 1988* (Cth), and any subsequent legislation that alters, repeals or replaces such legislation and all other equivalent laws and regulations relating to the regulation and enforcement of data protection and data privacy in any country.

### **Data Subject**

any natural person whose **Personal Information** has been either collected, stored, or processed by or on behalf of an **Insured Entity** or **Corporate Superannuation Trustee**.

### **Information Commissioner**

an Information Commissioner of the Office of the Australian Information Commissioner or position that replaces such a role under laws and regulations relating to the regulation and enforcement of data protection and data privacy in Australia and any equivalent position in any jurisdiction.

### **Information Holder**

a **Third Party** that:

- (i) an **Insured Entity** or **Corporate Superannuation Trustee** has provided **Personal Information** or **Corporate Information** to; or
- (ii) has received **Personal Information** or **Corporate Information** on behalf of an **Insured Entity** or **Corporate Superannuation Trustee**.

### **Personal Information**

any information relating to an identified or identifiable natural person.

**Personal Information** includes a natural person's name, online identifier, telephone number, credit card or debit card number, account and other banking information, tax file number, medical information, or any other information about a natural person protected under **Data Protection Legislation**, including but not limited to "personal information" or "sensitive information" within the meaning of the *Privacy Act 1988* (Cth).

### **Privacy Event**

- (i) a **Breach of Confidential Information** by an **Insured Entity**, **Corporate Superannuation Trustee** or an **Information Holder**; or
- (ii) a failure by an **Insured Entity** or **Corporate Superannuation Trustee** to notify a **Data Subject** or any **Regulator** of an unauthorised disclosure or transmission of **Personal Information** for which the **Insured Entity** or **Corporate Superannuation Trustee** is responsible in accordance with the requirements of any **Data Protection Legislation**.

### **Regulator**

an **Information Commissioner** or statutory or government body established pursuant to **Data Protection Legislation** in any jurisdiction and which is authorised to enforce statutory obligations in relation to the handling, use and disclosure of **Personal Information** (or, where relevant, **Corporate Information**).

### **Security Failure**

- (i) any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a **Company Computer System**, including that which results in or fails to mitigate any:
  - (a) denial of service attack or denial of access; or,
  - (b) receipt or transmission of a malicious code, malicious software or virus;
- (ii) the loss of **Data** arising from the physical theft or loss of hardware controlled by an **Insured Entity** or **Corporate Superannuation Trustee**; or
- (iii) the unauthorised reprogramming or corruption of software (including firmware) which renders a **Company Computer System** or any component thereof non-functional or useless for its intended purpose.

### **Third Party**

any entity or natural person except:

- (i) any **Insured Entity** or **Corporate Superannuation Trustee**; and
- (ii) any other entity or natural person having a financial interest in the operation of an **Insured Entity** or **Corporate Superannuation Trustee**.

**All other terms, exclusions and conditions of this policy remain unaltered.**