InsightCFS Data Security Policy

This policy should be read with specific raffle or fundraising campaign conditions and website terms of use where relevant.

This policy concerns the security provided by Insight to facilitate payments from contacted persons and supporters ("you") to charity clients of Insight for raffle and fundraising campaigns. This policy applies to the Insight entities set out below ("Insight" or "We" or "our"), any appointed suppliers and relevant staff involved in sales and payment processing. We may update and change these conditions from time to time.

1. Transaction purpose and authority

Personal and payment data is received for the purpose for which it was provided as agreed by you. You must authorise us to use payment information for purchases.

2. Related Agreements

All credit card, cheque, direct entry (direct debit) and BPay payment processing services are provided by Westpac Banking Corporation. Post BillPay services are provided by Australia Post under license from Westpac. All bank fees for successful transaction are paid by InsightCFS.

We provide security for the payment data as described for each method and generally for all data as set out in Schedule A. In the event of an actual or suspected data loss Insight follows the processes in the InsightCFS Data Breach policy.

Payment processing and data management may be affected by our service agreements with Westpac Banking Corporation for the supply of each banking service, merchant agreements for each client, Westpac Online service agreements, card payment acceptance agreements and Insight's client contracts. Use of your card and accounts are also subject to your agreements with your bank.

3. Privacy

Banking data is regarded as personal information for the purpose of the Privacy Act 1988. You may contact us and enquire what payment data we hold, and you may correct or add to that payment data as well as delete it as necessary. In summary banking data is only shared with Westpac for a purchase. Data may pass through service entities facilities e.g. website hosting services under secure conditions.

4. Storage

Purchase transactions and payment references must be retained for reference, audit and record keeping as required by raffle or donation laws and rules for between 3 and 7 years. At the end of that period payment particulars are deleted.

5. Processing

Credit or debit card payment information is always submitted to Westpac Bank as soon as practical for card present, online purchases or telephone order sales. We receive from Westpac a masked card number, unique sequence ID used for confirmation of receipt of the card details, confirmation of any authorised payment and any subsequent payment or communication.

Direct Entry banking is conducted by us for each client charity. Clearing funds for valid entry in a lottery may take up to 5 days. Insight captures BSB and account numbers in an encrypted form from cheques to verify payment, reconcile payments and for any subsequent consented payments.

Insight is permitted to register credit and debit cards for payment without expiry date or CVV number as a result of our supervised sales environment. We will normally not contact you to update expiry dates. All recurring and further payments lead to email or mail confirmation of that further raffle entry purchase.

Any payment faults or need for correction is referred to you. We may ask you to provide some form of identification.

6. Fundraising Campaign

We are unable to cancel or refund any valid payment for a completed raffle. Cancellation or amendment of participation in any raffle can be done at any time up to the draw date. Nothing here is intended to limit your rights to object to payments directly to us or via your bank.

7. Payment Conditions

Payment identifiers including sequence IDs (or tokens), account numbers and payment references are retained by Insight in a masked or partial format for reference and for use at your direction on any additional charity raffle campaign for which we may be engaged. Complete account numbers may be decrypted where required for identification purpose.

8. Responsibility and Liability

You will not be liable for losses resulting from unauthorised transactions made using our payment services where it is clear that you or an authorised user of your accounts, have not contributed to the loss.

You will be liable for losses resulting from transactions which are carried out by you, a user or by another person with the knowledge and consent of you or of any user.

If you see a transaction or payment which you dispute or do not understand which relates to Insight or its clients, contact us or your bank. Any unauthorised transaction will be refunded and investigated. 1300 365 896 info@insightcfs.com.au

Loss in this agreement is limited to the value of the transaction, which was processed, and fees directly related to that. We are not liable for any consequential loss or damage you suffer as a result of using the payment services, other than due to any loss or damage you suffer due to our negligence or in relation to any breach of a condition or warranty implied by law in contracts for the supply of goods and services and which may not be excluded, restricted or modified at all or only to a limited extent for example by the Australian Consumer Law.

9. Service Providers

Payment Services described in this Policy are provided by the following Insight related entities: Insight Holdings Consolidated Pty Ltd, Insight PSS Pty Ltd and D-Debit Pty Ltd.

Schedule A. Data Security Arrangements

Description of the technical and organisational security measures implemented by InsightCFS:

A. All credit card payment records are captured directly to the bank or card processor servers via secure encrypted sessions. No payment records are retained by us.
B. Payment Data (Primary Account Numbers or PANs) such as card and account numbers are transferred via secure encrypted link to Westpac and reference numbers (token) and maskedidentifiers are returned in the same manner.
C. Customer data is stored in off-site data centres under secure physical conditions.
D. All transfers of PANS to and from that data centre, for example to clients are made using secure VPN connections for direct transactions (eg live calling) or in an encrypted form by SFTP or FTPS
E. Access to payment data is limited as limited as possible, restricted to our sales staff, Banking/customer service staff and IT staff. Sales staff have one contact with PAN data at payment or for data entry under supervised conditions, customer and banking administration staff only access masked PAN or the initial collection from the customer and IT have wide access limited to their specific development and system supervision roles.
F. Physical records of PAN data are processed under secure conditions and the completed paperrecords stored on site prior to destruction.
G. All devices using customer data use updated Windows 10 Pro and run current virus checkers. Firewalls are used in all data collection environments such as at the data centre and by recipients of bulk data.
H. All Insight servers and PCs are updated for security patches as soon as released.

This policy was prepared on 13 April 2021 and reflects the policy and processes applied since 2011.

This policy is to be reviewed on 30 November 2021 and each year.