Policies & Documents

# Privacy Policy

## Statement of Affirmation

Identity Care Australia & New Zealand Ltd. (IDCARE) affirms its commitment to the laws and regulations of Australia and New Zealand in relation to Privacy, including Australian Privacy Principles, Guidelines and Best Practice

## Definitions

Clients – individuals that engage IDCARE for the provision of our services, whether the service is our free community service or a cost-recovered paid premium service.

IDCARE – means Identity Care Australia & New Zealand Ltd. (ABN 84 164 038 966) a not-for-profit and registered Australian charity.

Law Enforcement and National Security Agencies – these are agencies that are referred to in legislation as performing an enforcement or intelligence function on behalf of their State and/or Nation.

Members – a member of IDCARE is an organisation that has subscribed to receive our services for a nominated period of time. Members receive periodic reporting from IDCARE on issues, trends, organisation and market performance, and insights on how to enhance their response to clients that confront identity and cybercrime.

Personally Identifiable Information - in this privacy policy means any information from which your identity is apparent or can be reasonably ascertained.

Premium Services – means a service provided to individuals that includes consent to advocate and take necessary identity and cyber security repair actions on behalf of that individual client

## Primary Object and Business Purpose

IDCARE engages with individuals and organisations on highly sensitive issues involving the loss or theft of personal information, victimisation from deception, the exploitation of devices, and related concerns. The primary object of IDCARE that directs our business purpose is to represent the individual interests of identity theft and cybercrime victims through a number of activities, including raising awareness, education, building the capacity of organisations to respond to identity theft and misuse events, and directly supporting individuals in providing them with practical knowledge on what to do in response to an event and counselling support.

IDCARE does not refer to individuals or organisations as "victims". Individuals are known by IDCARE to be our clients and organisations are known by IDCARE to be our members.

## Collection of Personally Identifiable Information

Through the provision of IDCARE's specialist services our organisation may collect personally identifiable information, such as name, email address and other contact information. At times clients and organisations volunteer personal information without IDCARE requesting such. When this occurs, IDCARE will safely destroy such information where it is determined not to be necessary for the conduct of our business purpose.

IDCARE through the provision of our specialist services may collect derivative information that third parties, if communicated, may be in a position to determine the identity of IDCARE's client. For example, if IDCARE's client experiences a fraud event that relates to a specific monetary value at a specific time involving a specific organisation, whilst IDCARE may not be able to determine the identity of the client, the organisation involved in such a fraud on their products or services may. In such instances IDCARE will take all reasonable efforts when communicating information to third parties to remove this risk where consent to share with third parties about the specifics of the matter has not been received by the Client.

## Consent to Share

IDCARE is funded by organisations across the public and private sectors. This enables IDCARE to provide the community with a free support service. Our funding comes from the ability for IDCARE to report back to "member" organisations key trends and issues, including feedback on how their own customers have been treated and the impacts their organisation is having on the community. IDCARE provides such information in a form that is anonymous and in a way that seeks to remove the risk that the third party receiving such reports cannot identify the individual client, unless that client has given IDCARE express permission to share such feedback on their behalf.

## Advocacy & Premium Services

In addition to our free community support service, IDCARE can offer individual clients and members the opportunity for our organisation to advocate on behalf of the client. This service is a service whereby IDCARE is provided consent by the individual client to act on their behalf to assist in the repair of their identity. The service is a cost recovery service and therefore requires such individuals to make payment and provide personally identifiable information to IDCARE in order for IDCARE to perform this service. Payment is made via a third party payment processing platform. 128-bit encryption is used in the processing of such payments and at no point does IDCARE collect, store or share such payment information. Users of this service must agree to the terms and conditions of the third party payment platform including their own Privacy Policy (a relevant link has been provided on this payment gateway). IDCARE disclaims liability for any breach of such information in the use of the third-party payment platform. Whilst IDCARE reviews all of our service provider Privacy and Data Breach response capabilities, IDCARE cannot guarantee the security of such a provider and their protection of your payment information. Of course IDCARE will provide all reasonable assistance in response to any such event that the third-party payment platform has been breached where this is drawn to our attention.

## Sharing of Personally Identifiable Information with Third Parties ("Sharing Provision")

IDCARE may share personally identifiable information with third parties, such as law enforcement, national security, and other identity repair response organisations in the following circumstances:

- Where the individual has consented for IDCARE to share such information; and/or
- Where it is assessed by IDCARE to be a situation where an individual has an immediate threat to their life (for example, a client is assessed to be at imminent risk of self-harm and IDCARE reports this instance to local law enforcement or another service provider to conduct a physical welfare check); and/or
- Where IDCARE has been issued with a subpoena, warrant or related legal request from a Court or relevant law enforcement body; and/or
- Where IDCARE believes such information may be necessary for the enforcement of the laws of any Australian State or Territory, the Commonwealth or New Zealand in relation to an alleged serious crime or offence (where the alleged offence is punishable by imprisonment for a period exceeding 12 months).

## Using Personally Identifiable Information

IDCARE uses personal information in accordance with our "Sharing" provisions under this Policy. In almost all cases, IDCARE will use Personally Identifiable Information in order to provide its Premium Service for individual clients upon receiving consent for such a service by that individual. IDCARE's Premium Service can involve acting on behalf of consenting clients by sharing with specific third parties that are necessary to engage for the appropriate repair of compromised or misused personally identifiable information. Such third parties may include credit reporting agencies (such as Equifax, Experian, Dun & Bradstreet, the Tasmanian Collection Service, and Centrix), the Australian Cybercrime Online Reporting Network (ACORN), CERT Australia and CERT New Zealand, AusCERT, NetSafe, the Office of the eSafety Commission, telecommunications carriers and service providers, financial institutions, law enforcement agencies, national security and intelligence agencies, and other relevant third parties necessary for the effective response and repair of compromised personally identifiable information relating to that individual.

IDCARE also provides reporting services to the public, business, government and not-for-profit third parties. Unless covered under the "Sharing Provision" of this policy, IDCARE will take all reasonable steps to ensure that such reporting services shall not include the sharing of personally identifiable information. Such reporting will be restricted to anonymised events where the risk of derivative identification has been managed. Such reporting can include the presentation of aggregate information on current and emerging trends, market sentiment, organisational and technological vulnerabilities, non-identifiable statistical information collected and analysed from IDCARE's National Case Management Centre. IDCARE may use ratings and scoring provided by individual clients to develop statistical scores and performance measures on the activities of business, government and not-for-profit organisations at individual organisation level, market segment level, industries and sectors. IDCARE may also use such performance measures as a means to attempt to motivate policy and regulatory change through specialised, but anonymised, reporting, workshops, media engagement, and related communications.

## Media

Often IDCARE is asked to comment in the media about current and emerging trends. This can include instances where IDCARE clients have been engaged by the media (either unilaterally or by request). IDCARE will refuse to comment about specific client matters to the media unless consent is provided by that client and IDCARE believes that the process of consent is ethical, consistent with our organisation's own Code of Practice, and the Codes of Practice of relevant professional bodies (such as the Australian Counselling Association).

## Personally Identifiable Information Protection

IDCARE will take all reasonable attempts to protect personally identifiable information collected by clients. Our core service of providing free community support does not require IDCARE to collect any personally identifiable information and care has been taken to ensure that where such information is collected, it is absolutely necessary to do so.

At least annually IDCARE undertakes risk assessments in relation to our collection, storage, sharing, and destruction of personal information (guided by the ISO 31000 standard on risk management). IDCARE also performs Privacy Impact Assessments when proposing the delivery of new community services to evaluate the nature of the risk, strategies for mitigation, and our on-going responsibilities in meeting Australia and New Zealand's privacy legislation and regulation.

## Retention of Personally Identifiable Information

IDCARE only retains personal information for as long as is it is required for the purposes for which that information may lawfully be used (for example, employee and volunteer details, next of kin information etc). Client information is anonymised and retained for statistical analysis, such as time series analysis. This information is backed-up periodically and stored in a non-networked or Internetenabled environment within IDCARE.

## Data Breach Response

IDCARE knows too well that data breaches can impact any organisation. IDCARE reviews and tests periodically our data breach response policy and plan. Given the nature of our service, we know IDCARE is a likely target of identity and cyber criminals. We take measures to address this risk and continue to review our practices. In the event that personally identifiable information has been breached, IDCARE will take all reasonable steps necessary to notify impacted individuals where such events are assessed to create the potential for serious harm and offer such individuals support, such as IDCARE's Premium Support Service. The Premium Support Service will include the facilitation of a number of identity repair actions, including, but not limited to, credit report protection, monitoring of compromised identity information, and counselling support.

## Access, Correction, Feedback and Complaints

If you wish to access information collected by IDCARE relating to your circumstances, seek correction of information held about these circumstances, have your personally identifiable information destroyed, or IDCARE Copyright ©2017 Page 4 of 6 make a complaint about how we have dealt with your matter, please send a written request, including your case number, to:

Privacy Officer IDCARE PO Box 412 Caloundra QLD Australia 4551

Requests may also be emailed to privacy@idcare.org with the words "Attn: Privacy Officer" in the subject line. To assist IDCARE in responding to your request we would be grateful if you could provide your IDCARE Case Number (if relevant) and the estimated date of your engagement with IDCARE.

## Website and Social Media Traffic Monitoring

IDCARE does monitor website and social media traffic via a third- party web and social media analytics platform. Due to the dynamic nature of this environment IDCARE is able to access reports from this third party to inform our organisation of usage statistics to assist us in planning and fixing the quality and compatibility issues around the following:

- performance of site downloading time,
- functionality of the site, Property rates notice
- review to rule out the broken links,
- traffic analysis to give report to broken links,
- prevention and awareness campaign development,
- feedback of visitor which is beneficial for the enhancement of the site.

To achieve the above, IDCARE may collect, hold, and use statistical information about visits to help us improve the site, for instance:

- IP address
- The search terms used
- The pages accessed on our site and the links clicked on
- The date, time and duration of the visited the site
- The referring site (if any) through which the user clicked through to our site
- The user's operating system (eg Windows XP, Mac OS X)
- The type of web browser used (eg Internet Explorer, Mozilla Firefox)
- Whether the user access the site using a computer, tablet or smart phone

The data collected is aggregated and is not personally identifiable. IP addresses are masked so that they cannot be used to identify individuals. Our web analytics will also respect any "do not track" setting you might have set on your browser.

To improve your experience on our site, we may use 'cookies'. A cookie is a small text file that our site may place on your computer as a tool to remember your preferences. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website.

Our website may contain links to other websites. Please be aware that we are not responsible for the privacy practices of such other sites. When you go to other websites from here, we advise you to be aware and read their privacy policy.

Our website uses Google Analytics, a service which transmits website traffic data to Google servers in the United States. Google Analytics does not identify individual users or associate your IP address with any other data held by Google. We use reports provided by Google Analytics to help us understand website traffic and web page usage.

By using IDCARE's website (www.idcare.org), each user consents to the processing of data about them by Google in the manner described in Google's Privacy Policy- external site and for the purposes set out above. A user can can opt out of Google Analytics if they disable or refuse the cookie, disable JavaScript, or use the opt out service provided by Google- external site.

IDCARE also uses interfaces with social media sites such as Facebook, LinkedIn, Twitter and others. If you choose to "like" or "share" information from our website(www.idcare.org) through these services, you should review the privacy policy of that service. If users are a member of a social media site, the interfaces may allow the social media site to connect their visit to this site with other Personal Information.

## National Identity Lab Activities

IDCARE operates a National Identity Lab that takes anonymised data from our National Case Management Centre to undertake research and analysis to assist in prevention, awareness, detection and response capabilities. The anonymised data can include de-identified case information, performance scores from IDCARE's testing of the response environment, and response plan data. At times IDCARE sponsors researchers to use this anonymous data to assist them in undertaking research that IDCARE assesses to be of potential direct benefit to the community in reducing the harm from identity and cybercrime. Clients that have consented to participate in future research conducted by the National Identity Lab may be re-engaged by IDCARE or a visiting researcher working within IDCARE's environment. Each research project must have received ethics approval from the relevant tertiary sector institution and consent to participate in such research must be obtained by each participating client on re- engagement. A decision to participate or not in such research activity will have no bearing on whether such clients are eligible to receive ongoing support by IDCARE. It is a condition upon sponsoring external researchers that such research must demonstrate utility for the community, either through the provision of content for IDCARE Alerts, Fact Sheets, Bulletins or other direct prevention, detection and response measures. Failure of a sponsored researcher or institution to demonstrate this value may result in having future requests for support from IDCARE denied. Access to such data may only be provided on a user-fee basis, only for a specific purpose, and only on the condition that the research meets agreed priorities. Any revenue generated from such activity must be reinvested into IDCARE's community support activities, such as staff costs in running the National Case Management Centre.