Data Security Policy

February 2023

Version 1.4

Notitia

Context

This data security policy (”policy”) will help you understand how Notitia Pty Ltd (”Notitia”,”us”, ”we”, ”our”) handle and securely protects the data and information you provide to us when you engage with Notitia for professional services or product(s). This policy additionally includes information generated when you visit and our website(s) www.notitia.consulting; www.notitia.com; www.notitia.com.au (”website”). We reserve the right to change this policy at any given time.

Guiding Principles

- Notitia aims to manage data security risks posed to those we interact with including our staff and our clients.
- This document defines how we approach data security, including the relevant policies and procedures in place. As this document is external-facing, we have omitted specific details to minimise our threat exposure.
- Notitia takes client data incredibly seriously. We don’t look to own, reuse, or profit from holding client data. Any use of client data is expressly aligned to a specific client engagement, or to provide an ongoing service to a client.
- Where we do have to handle or store client data, we ensure that our policies and procedures are in line with leading Managed Service Providers and industry benchmarks. Our policies are outlined below.
- Acceptable Use of Data:
    - Client data is only to be used for the purpose of delivering value to a client.
    - This includes but is not limited to, Notitia providing services and products for the client.
    - Client data is never onsold, shared, aggregated, transferred, retained, analysed or any other meaningful work performed without the express written permission of our client(s).
    - Where Notitia has a copy of any client data at the end of the engagement, this data is securely destroyed and no client data is retained by Notitia after the cessation of an engagement.

Practical

Password Policy:

- Notitia enforces a complex password policy.
- Passwords are never shared across the organisation.
- Password management for common client environments are stored securely via a Password Manager application.
- Password ageing is incorporated into our Password Management activities together with password length, complexity and expiry which is determined by the security and complexity of the client, the data, the application and the environment.
- Two-factor Authentication is enforced where technologically possible.

Email Policy:

- Notitia uses a secure, encrypted cloud email provider with all email data stored locally in Australia.
- Our corporate emails are tracked, logged and periodically audited to ensure compliance.
- Staff are instructed and agree to comply with only using corporate emails for work.
- Our email systems actively monitor and prevent phishing, spam and other malicious software or attacks on our systems.
- Awareness and education of email cybercrime is conducted within Notitia.

Social Networking:

- Use of Social Media and Networking is required to be in line with our Social Media Policy
- References to clients on Notitia-owned and managed social media platforms only occur with express permission from our clients.

- Client data is never shared or published online.
- Access to Notitia social networking accounts is controlled and limited to specific individuals within the organisation.
- Employee social media accounts, and use of social media by our employees does not constitute a representation of Notitia.
- Any opinions expressed in the social media post or engagement belong solely to the author, and do not represent the views of Notitia.

Software Copyright and Licensing:

- Notitia maintains records of all software in use, including a repository of active licences across the organisation.
- The use of unlicensed software is strictly prohibited, and violates the terms of our employee's employment agreement(s) and required code of conduct.
- As part of our audit process, ad-hoc scanning of any Notitia-owned device occurs to ensure software copyright and licensing compliance.

Auditing:

- Notitia maintains a suite of technology platforms that enable real time alerting, monitoring, and auditing of our technology environment.
- We routinely audit our environment to expose access attempts, changes to system configuration and network activities.
- Our full suite of auditing processes and approaches is confidential in nature, and evolves to reflect the changing threat landscape and controls environments that are appropriate for handling the specific sensitivity of client data.

Incident Reporting:

- Where an incident occurs, such as a breach of our security or potential impact to client data, Notitia uses an Incident Reporting system to capture any incident, and our response.

- Breaches are taken extremely seriously, and are resolved by Notitia's leadership team and our managed service provider's cyber security team.
- Mobile Device Management: Use of endpoint management and Mobile Device Management (MDM) through leading cloud identity management platform providers. All of our devices are able to be remotely deactivated in the case of loss or breach.
- Any use of corporate emails on personally-owned devices such as BYO mobile devices are able to be remotely monitored, accessed and information securely erased.

Backup, Recovery and Disaster Recovery (DR):

- Notitia does not store data locally on any device. We have a cloud-first policy for backup and data storage.
- Backups are stored through a variety of machine image snapshots, document rollbacks, and environment images.
- All data is stored off-site and encrypted, via our cloud partners.
- In the case of disaster recovery, Notitia has procedures in place with leading cloud vendors to provide disaster recovery.

Encryption:

- All Notitia devices are encrypted by default. We use hard disk encryption and file encryption.
- Any traffic in and out of cloud environments is protected in transit with SSL and protected at ingress and egress with HTTPS. This ensures that it is unreadable by any third party that intersects the data.
- Where Notitia handles Personally Identifiable Information (PII) data, we undergo a process of de identification, using hash keys to obfuscate any personally identifiable information.

- Any PII is held securely by Notitia for the shortest amount of time possible, and provided back to clients as soon as possible, and securely deleted as soon as possible.