Nous Information Security and Privacy

Information security and privacy – general

Nous is proud of being a purpose-driven organisation. Clients are our first priority. Our Information Security Framework has been implemented to support the delivery of our consulting services and to ensure Nous safeguards your interests and continues to deliver positive influence, now and into the future.

The objectives of the Information Security Framework are to ensure that:

- **Our people are adequately equipped to make the right decisions** when collecting, storing, processing, sharing and/or destroying information and when using Nous' IT equipment or permitted personal devices (e.g., BYOD).
- **Our processes and technology are operating as efficiently and effectively as practicable** to promote productivity and for Nous' business continuity and resiliency.
- **We continuously improve** using globally recognised best practices standards (e.g., **ISO 27001** and **NIST Cyber Security Maturity**), client specific requirements (e.g., Government agencies) and relevant legislation (e.g., **privacy and anti-spam acts**) as the baselines, so that we can be appropriately transparent with clients and other external stakeholders on information security matters.
- **Subcontractors, and other third-parties** who may have access to personal information (including health) and other client sensitive information are provided clear information security expectations and are monitored accordingly.
- **Information security incidents and vulnerabilities are addressed** in a timely manner, and in adherence with applicable data breach notification requirements under legislation.

Information security and privacy – on projects

Nous is experienced in collecting, processing and analysing data, and sharing meaningful results and reports with our clients. We use a range of digital tools to enable these activities and the following is an inexhaustive list of some of the tools we use.

- s 47(1)(b) [redacted] and s 47(1)(b) [redacted] are used to store and collaborate on project documentation, data and reporting. Information is securely stored and processed in the s 47(1)(b) [redacted]
- s 47(1)(b) [redacted] is also used for video conferencing, facilitating online workshops and interviews.
- s 47(1)(b) is an s 47(1)(b) [redacted] which enables participants to collectively s 47(1)(b) [redacted] and other s 47(1)(b) [redacted].
- s 47(1)(b) is an easy-to-use s 47(1)(b) [redacted] s 47(1)(b) [redacted] (real or virtual). s 47(1)(b) is particularly useful for s 47(1)(b) [redacted] s 47(1)(b) [redacted] where an s 47(1)(b) [redacted]
- s 47(1)(b) is an intuitive, yet sophisticated s 47(1)(b) [redacted] used to securely s 47(1)(b) [redacted] s 47(1)(b) [redacted], to s 47(1)(b) [redacted].

We are willing to explore any other client preferred digital tools throughout the project.

Adopting a risk-based approach, Nous has implemented the following safeguards to protect high-risk / sensitive information, such as personal information, health information and/or any other information that is sensitive to ASIC and/or the project.

- Nous performs risk assessments on the third-party vendors of the digital tools that we use against best practices (e.g., ISO 27001, GDPR compliance, SOC 2 reports, etc) to minimise risks of data leaks.
- All digital tools are configured with user access controls on a strictly need-to-know basis.
- Project Information Risk Assessments (PIRAs) provide an auditable trail for each project on how any personal or client sensitive information was collected, stored, processed, shared, archived and/or destroyed on that project. PIRAs identify what types of personal or client sensitive information were involved in the project, which IT applications were used on the project, and if a subcontractor may have handled personal or client sensitive information during the project.

Information security – technical

IT and building security

Nous uses s 47(1)(b) [redacted] for email communication, s 47(1)(b) [redacted] and s 47(1)(b) [redacted] for document management and collaboration. This information is stored securely and processed within the s 47(1)(b) [redacted]

All data for Australian, UK and Canadian clients are stored and processed in Australia, the UK, or Canada respectively on s 47(1)(b) [redacted], which therefore meets data sovereignty requirements for each country (more information is available here: s 47(1)(b) [redacted]).

s 47(1)(b) [redacted] also complies with an extensive range of global, industry and regional information security standards: s 47(1)(b) [redacted] including: ISO 27001, UK GDPR, Canadian Privacy Laws, UK Cyber Essentials Plus, UK G-Cloud and Canadian OSFI

s 47(1)(b) [redacted] is installed across s 47(1)(b) [redacted] s 47(1)(b) [redacted] s 47(1)(b) [redacted] Nous performs s 47(1)(b) [redacted] and s 47(1)(b) [redacted] and s 47(1)(b) [redacted] for s 47(1)(b) [redacted] s 47(1)(b) [redacted], while using s 47(1)(b) [redacted] s 47(1)(b) [redacted].

Nous engages an independent cybersecurity firm, to s 47(1)(b) [redacted]

During the COVID-19 pandemic, Nous enacted a "hybrid working" model to support staff when working remotely or at one of Nous' offices. Access to Nous cloud software and data requires authentication via s 47(1)(b) [redacted]

Physical security

Offices are secured by s 47(1)(b) [redacted] and staff are required to use s 47(1)(b) [redacted] to enter the office. Building management s 47(1)(b) [redacted]. All staff are required to s 47(1)(b) [redacted] s 47(1)(b) [redacted]

Data capture

We use consistent data management approaches which include standardised templates for data capture, processing and reporting during all project components.

Data storage and back up

s 47(1)(b) stores information in a redundant environment with strong data protection capabilities to enable availability, business continuity, and rapid recovery. s 47(1)(b) has multiple levels of data redundancy, such as redundant disks to guard against local disk failure and continuous, full data replication to an alternative data centre. Details of s 47(1)(b) worldwide uptimes are available here: s 47(1)(b) [redacted]

Data breach response

Nous takes the protection of data very seriously and we have implemented various measures to protect the sensitive commercial and personal information in our possession.

In the event of a data breach, we recognise the importance of moving quickly to identify and contain the data breach and notify any relevant parties. Therefore, Nous has implemented a Data Breach Response Plan which we regularly test to ensure Nous' Incident Response Team is adequately prepared in the event of an actual data breach.

The Data Breach Response Plan clearly outlines roles and responsibilities for s 47(1)(b) [redacted].

As soon as becoming aware of an actual or suspected data breach, our Incident Response Team will s 47(1)(b) [redacted]

- [redacted]
- [redacted]

We will subsequently keep our clients informed of the incident and work with them, and other third parties if required, to contain and resolve the data breach. Nous will also notify any affected individuals and the relevant supervisory authority in accordance with our obligations under applicable laws, including adhering to the strict timing requirements.

Certifications and compliance with ICT standards

On UK-specific certifications: Nous currently holds Cyber Essentials certification from GCHQ's National Cyber Security Centre.

On ISO:27001 certification: s 47(1)(b), including s 47(1)(b), is ISO27001 compliant. Although Nous is not currently certified, we align our information security management practices with ISO27001. We also undergo regular risk and information security maturity assessments against the s 47(1)(b) [redacted].

s 47(1)(b)**:** Nous has implemented the s 47(1)(b) of the s 47(1)(b) [redacted]

Insurance

Nous currently holds Cyber Defence Insurance Policies in Australia, UK, and Canada.

Data security training

Nous staff are required to undertake annual information security and privacy training, supplemented with communications to staff throughout the year with information security updates and attack simulations (e.g. phishing and weak password cracking).

Staff are trained in how to identify and report suspicious activity and insider threats, how to improve access management practices (including screen-locking and password complexity) and the privacy and security requirements under Australian, UK and Canadian regulatory regimes.

Confidentiality and ethics

Nous has a strict privacy policy and educates its staff on the importance of designating and managing sensitive information. Nous is accustomed to managing highly sensitive data. Our project establishment methodology uses a step-by-step process to initiate new projects which includes formally defining the 'need to know' team members, securing project workspaces and enforcing role-based access rights. Nous will not share any information with third parties unless agreed with clients.

Policies for clients

Nous has the following client facing information security policies in place:

- Information Security
- Information Classification and Handling
- ICT Acceptable Use
- Identity and Access Management
- Bring-Your-Own-Device
- Remote Access
- Third Party Information Security
- Privacy Policy
- Data Breach Response Plan.

Australian privacy compliance

Nous complies with the Australian Privacy Act 1988 Cth and has applied the 13 Australian Privacy Principles to how we:

- Collect, use and disclose personal information.
- Ensure our governance and accountability of protecting personal information.
- Ensure integrity and enable correction of personal information.
- Enable individuals to access their personal information in our possession.
- Keep personal information secure from misuse, interference or unauthorised access, modification or disclosure.
- Destroy or de-identify personal information.

Australian Government Defence Industry Security Partner (DISP)

Nous has successfully attained membership of the Australian Defence Industry Security Program (DISP). To achieve this membership, we have demonstrated to the Defence Industry Security Office (DISO) our ability to minimise security risks and raise our level of security protection across the security categories of governance, personnel security, physical security, and information and cyber security.

Attainment of DISP membership means Nous is approved by the Australian Government to securely host, store and transfer information up to the level of ***OFFICIAL: Sensitive***.

Some of Nous' key information security measures include:

s 47(1)(b)