# Information Security Policy

## Information Security Organization

Information Security will be managed by the following personnel:

- Karl Holub, Technical Lead
- Kevin Kallmes, CEO
- Kathryn Cowie, Operations Lead
- Stephen Mead, Lead Engineer
- An external cybersecurity consultant, who has already been vetted and interviewed by Nested Knowledge, will be hired as an independent contractor if the needs of our information security organization expand.

### Review:

All policies will be reviewed on an annual basis or earlier, should a major system changed occur.

### Personnel changes

In the event of a change in role, a departure, or a new hire, oversight of the affected security policies will be transferred to the new information security personnel. Management of information technology systems will be transferred to the appropriate engineer. Barring no sudden change, the transition will take place over two to eight weeks and will include training, knowledge checks, and progressively increasing responsibility over policies.

# Data Protection Plan

## I. Purpose

The Data Protection Plan helps us prepare to identify and protect personal data. A data protection impact assessment (DPIA) is required for projects where data processing is “likely to result in a high risk to the rights and freedoms of natural persons.” The plan here outlines our procedure for developing a DPIA.

## II. Scope

This plan applies to all Nested Knowledge employees, and all contractors, consultants, temporary employees and business partners.

High-Risk personal data includes:

- location and behavior data
- systematically monitoring a publicly accessible place on a large scale
- personal data related to “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health or data concerning a natural person’s sex life or sexual orientation
- data used to make automated decisions about people that could have legal (or similarly significant) effects
- children’s data

# III. Policy

## Data Protection Officer (DPO)

The DPO, responsible for reviewing and approving data processing projects, is Karl Holub.

In brief, the DPO:

- Is made available for all product & support teams, for reporting & planning any changes to data processing
- Monitors for changes that are of consequence to our data processing policies, including:
  - Code changes and releases
  - Third party vendors & subprocessor additions
  - Internal tooling & workflow changes
- Maintains records of compliance, associated directly with the issue tracker, processor record
- Reports to the CEO on activities and compliance on a regular basis

**DPO Email:** karl.holub@nested-knowledge.com

## Data Protection Impact Analysis Plan

Nested Knowledge will fill out a data protection impact analysis before processing any high-risk personal data.

#### We will take the following steps:

1. **Identify the need for a DPIA**
    1. Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarize why you identified the need for a DPIA.
2. **Describe the processing**
    1. **Nature of the processing:** How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

    2. **Scope of the processing:**what is the nature of the data, and does it include special category or criminal offense data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
    3. **Context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
    4. **Purpose of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
3. **Consultation Process**
    1. describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organization? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
4. **Assess necessity and proportionality**
    1. **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
5. **Identify and assess risks**
    1. Describe the source of risk, likelihood of harm, severity of harm, and overall risk. Include associated compliance and corporate risks as necessary.
6. **Identify measures to reduce risk**
    1. Record options to reduce or eliminate risk, the effect on risk, residual risk, and whether or not the measure was approved.
7. **Sign off and record outcomes**
    1. The Data Protection Officers should sign off on risk-reduction measures and provide advice.

For templates to complete the above steps, refer to the ICO guidance

## High-Risk Personal Data

Nested Knowledge does not process high-risk personal data. Potential high-risk data types we may encounter in our industry include the following:

- Information on employee health and/or disability status.
- Information on employee ethnicity, race, religion, sexuality, or political beliefs.
- User location data and online behavior

Nested Knowledge values the privacy of our employee and users. We have no intention to process such data, but we will remain alert and develop a DPIA should our data processing plans change.

## Training

Employee training requirements are based on the data classification system. All employees and contractors will be provided with our data protection policy. Those who deal with confidential data, restricted use data, or high-risk personal data will be required to demonstrate understanding of our data protection procedures.

### Communicating Updates

As described in our Third Party Policy, we will notify users of changes to how their data is processed at least 7 days in advance.

# Backup Plan

## I. Purpose

The purpose of this policy is to ensure that data used within Nested Knowledge's systems is regularly backed up.

## II. Scope

This policy affects all employees and contractors of Nested Knowledge. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

This policy applies to all computer and communication systems owned or operated by Nested Knowledge and it's subsidiaries. Systems include company shared drives, purchased software, as well as access to the Nested Knowledge AutoLit review platform. Similarly, this policy applies to all platforms (operating systems) and all application systems. Reviews developed in the AutoLit software by parties external to Nested Knowledge are not covered in this policy.

## III. Policy

### Backup Procedures

Remote workers are responsible for ensuring that their remote systems are backed up on a periodic basis.

- It is recommended that all personal computers be backed up. Copies of the personal computer files should be uploaded to the Nested Knowledge shared drive. This provides for a more secure backup of personal computer-related systems where a local area disaster could wipe out

important personal computer systems.

### Backup Strategies

- Where a third party has been authorized to store backup media, a service level agreement (SLA) should be defined and documented, and in compliance with the IS Security Standards.
- Automated backup functions within software packages should be used where applicable.
- When a computer equipment is changed, consideration should be given to the backup media and data formats to ensure that they can still be restored.

### Database Back Ups

Backups are generated as database snapshots daily; transaction logs are streamed to storage and stored for 14 days (providing moment in time restoration within that window). Failure in either of these processes generates email alert to the technical lead. Database backups are fully exercised no more than every 3 months. Backups are retained 60 days. A failure in restoring a backup results in highest priority escalation with the development team on our product management software.

In addition to backups on our main cloud provider (AWS), we generate & store backups on a separate cloud provider (GCP) as a redundancy. These backups are generated every other day, retained 60 days, and exercised quarterly. Failure in the backup process results in email alert to the technical lead.

### Restoration

- Authorization to restore data from backup media that would overwrite existing production data must be obtained from Data Owners.
- Restoration of the current configuration must be within agreed recovery timescales
- Restoration of the AutoLit database is tested with quarterly by the development team. A successful restore requires taking a backup from stationary to deployed in our staging environment.
    - Backups are manually compared for validity against existing projects
    - Evidence of success backup is maintained internally, including time of test, verifiers, screenshots of successful staging deployment, and notes on any issues & remediations.

### Testing

Backup and restore procedures must be tested at least annually. Issues with backups identified should be documented and remediated.

# Revision History

| Author | Date of Revision/Review | Comments/Description |
|---|---|---|
| K. Cowie | 11/17/2021 | Initial Draft Completed |
| K. Holub | 12/13/2023 | Better defining DPO role |
| K. Kallmes | 11/19/2021 | Draft approved |
| P. Olaniran | 11/7/2022 | |

Return to Policies