Arda Terms and Conditions

Version 2.2 03-11-2026 Max van Eijden

Introduction

This document contains the terms and conditions for the use of the Arda security awareness service. This is a service produced and managed by Arda.

Need direct contact? Send an email to:support@arda.nl or call 085-4018487.

Arda
Statutory name: TSDA BV h.o. Arda
Chamber of Commerce: 62717413
Röntgenlaan 25 C
2719 DX Zoetermeer

Definitions

Term	Description
AP	Data Protection Authority
Arda	The Arda Security Awareness platform based on the ALE
AVG	General Data Protection Regulation (GDPR)
AWS	Amazon Web services, a cloud computing service by Amazon
CVD	Coordinated Vulnerability Disclosure
GCP	Google Cloud Platform
SAAS	Software as a Service, online software on a subscription basis
SLA	Service Level Agreement, an agreement containing arrangements regarding service delivery.
Arda	Trade name of TSDA BV registered with the Chamber of Commerce under number 62717413

Thingks	Trade name of TSDA BV
BUT	Arda Learning Engine, the learning environment on which Arda is based

Terms and Conditions

1: Arda applies the General Terms and Conditions as drafted by NL Digital, which you can find here.

2: Arda offers a learning environment in the field of information security. By using it, you agree to these terms and conditions.

3: Arda is software that you use via a modern browser. Arda uses the services of Amazon Web Services (AWS) and Google Cloud Platform (GCP). These services are hosted in Amazon's data centers in Frankfurt, Germany, and Dublin, Ireland. Arda sends notification messages and emails required for using the service.

4: Ardahas an availability of 99.95%, which is concluded under a Service Level Agreement. If the service does not meet expectations technically or in terms of content, you may send an email to support@arda.nl

5: Both the content of the learning modules and the technical structure are the intellectual property of Arda - the producer of Arda - and are protected by copyright.

6: How we handle data and personal data is described in the Arda Privacy Statement.

7: A component of Arda in combination with information security is the sending of so-called phishing simulation emails — emails attempting to obtain confidential data such as passwords. Arda will never store or share confidential information obtained from such emails with third parties such as an employer.

8: If you use this service on behalf of an employer, it is possible that your employer obtains information about your use of Arda, for example in the form of reports. These may include followed modules and results, points earned in games, or the number of clicked links in phishing emails.

9: Interaction and achieving results are rewarded with points and certificates. These points may be displayed on scoreboards visible to other users. Opt-out options can be found in the profile.

10: These terms and conditions remain valid as long as you have an account on Arda.

11: Arda creates its content with the utmost care. Arda cannot be held liable for any errors in the learning content or imperfections in the technical system.

12: Arda complies with Dutch and European law, meets the requirements of the General Data Protection Regulation (GDPR), and reports data breaches to the Dutch Data Protection Authority (AP) in accordance with the prescribed procedures.

13: If you have questions about these terms, experience a problem, or need help, you may send an email to support@arda.nl or call 085-4018487 and select option 1.

14: Upon request, we will send you the Arda security policy. This policy document contains confidential information that may not be shared with third parties without explicit permission. Arda is ISO27001 certified.

Application

The Arda portalis accessible at the following URL:
https://portal.arda.nl

More information about Arda can be found at:
https://arda.nl

Coordinated Vulnerability Disclosure

Arda contributes to increasing the resilience of Dutch businesses in the digital domain and thus to a secure, open and stable information society by providing engaging content and a learning environment. Naturally, Arda also finds it extremely important that its own ICT systems are secure and aims for a high level of protection. Nevertheless, it may occur that a weakness — also referred to as a vulnerability — is discovered in one of these systems.

If you have discovered a weakness in one of Arda's ICT systems, we would like to be informed so that the necessary measures can be taken as quickly as possible. Arda would like to cooperate with you to improve the security of its ICT systems. With this in mind, Arda applies the following policy regarding notifications of vulnerabilities you have identified in the Arda portal. You may hold Arda to this policy when you find a weakness in one of the systems.

We ask you:

- Send an email to support@arda.nl.If it concerns a serious vulnerability, send only an email without further explanation; we will then provide additional information to ensure secure communication.
- Provide sufficient information to enable us to reproduce the vulnerability.
- Not share this information with others until the vulnerability has been resolved.
- Handle this information responsibly.

What you may expect:

- Arda will not pursue legal consequences for submitted reports of vulnerabilities.
- Arda will treat communications confidentially and act transparently.
- Arda will mention your name as the discoverer if you so request.
- Arda will respond promptly and adequately to your report.
- Arda may issue a reward depending on the significance and quality of the report. This may range from a t-shirt to a reward of up to 500 euros.

We comply with the guidelines of the National Cyber Security Centre (NCSC) as described at: https://www.ncsc.nl/onderwerpen/cvd-beleid/cvd-beleid-opstellen