



Course Catalogue Engineering and ICT

EXCHANGE PROGRAMME

Digital Trust & Information Security 2026-2027

*University of
Applied Sciences*

Windesheim



Course summary
 VOE Code: V.ICTDTIS. ECTS credits: 30
 Level: Bachelor's degree (full-time) Semester: Autumn and Spring

Course Title	Multidisciplinary Security Project – Digital Trust & Information Security
Type	Compulsory
Learning competences	Security analysis and design; research; governance and risk management; multidisciplinary collaboration; professional communication; personal leadership.
Learning outcomes	The Minor Digital Trust & Information Security prepares you to work in a digital reality where technology, risk, human behavior, and regulation are inseparably connected. You will learn how to build trust in systems that are becoming increasingly autonomous, how to identify and manage risks in IT, OT, and AI environments, and how to help organizations operate securely, responsibly, and future-proof. In the Minor Digital Trust & Information Security students learn, in various phases, in collaboration with actual clients, to investigate the possibilities and solutions in cybersecurity and work on new applications using procedures, protocols, tools and technology. Conducting research, developing proof-of-concepts and/or building prototypes form a substantial part of most projects. The Minor Digital Trust & Information Security is one of the elective semesters of ICT. In these semesters, students learn to participate in projects in a professional working environment. This is done in multi-disciplinary teams for an actual client or a real-life setting. In this way, students learn from the professional environment, as well as other disciplines in the project. The feedback, evaluation and supervision focuses on preparing students as much as possible for the final graduation phase of the study programme.
Course content	The Minor Digital Trust & Information Security projects can vary considerably. Examples are developing security policies for businesses, researching future technologies such as autonomous vehicles, securing OT-environments or AI in different layers. In the Minor Digital Trust & Information Security every project is different, which means that the learning opportunities can vary as well. It is up to the student how they choose to shape the semester. To help the students with their projects, a number of workshops can be attended. Some of them are obligatory (e.g., project management, planning) and some are optional (scrum, game design etc.). The workshops are not graded individually, but are aimed to contribute to the succes of the specific projects.
Planned learning activities and teaching methods	Students work on a large project for 20 weeks. The project is done for an actual client or in a real-life setting. The multi-disciplinary student teams work on the project for 40 hours every week (Monday to Friday) at school or at the client's location. As part of the project there are project coaching sessions, workshops contributing to the project and regular presentations in which students share their obtained knowledge and progress.
Recommended or required reading and other learning resources / tools	Only freely-accessible learning materials are being used. When specific hardware of software is needed for your project, this will be provided.

Prerequisites and co-requisites	Two years of Bachelor's study experience in a related field and English-language skills at at least B2 level
Level	Advanced
Grading scale	Above expected level / At expected level / Needs work / Not assessable
Assessment methods and criteria	Students are coached in their project groups on a weekly basis. Workshops will contribute to the project's needs. The minor is based on programmatic assessment, meaning that there is no possibility of a resit.
Language of Instruction	English
Name of lecturer	Jan de Groot – J.D.de.Groot@windesheim.nl
Mode of delivery	Face to face, on campus and/or at the client's location.