

## Code of Conduct

### 1. Foreword by the Executive Board

This Code of Conduct serves as a framework for all the internal guidelines and the conduct of all the employees and supervisors of CISPA Helmholtz Center for Information Security (CISPA).

This means that the Code of Conduct is an overarching set of rules which is part of the compliance management system. It is intended to serve as a guideline for legally compliant, responsible conduct and thus protect CISPA, our employees and our partners from damage which could result from non-compliance with legal regulations and ethical and moral rules.

Our actions are based on respect, fairness, esteem, loyalty, security and frankness. CISPA's Code of Conduct set out below makes these principles clear.

The Executive Board expressly recognises this Code of Conduct and expects all CISPA employees to act in accordance with it.

### 2. Our mission

CISPA is a major research institution belonging to the Helmholtz Association of German Research Centers (HGF). It researches all facets of information security and, since its foundation, has evolved into one of the world's leading research institutions for IT security.

As a Helmholtz center, CISPA has the critical mass needed to provide a comprehensive, holistic treatment to the most pressing, fundamental challenges of cybersecurity research that exist in our age of digitalization. By combining cutting-edge, often disruptive foundational research with innovative application-oriented research, technology transfer and societal impact, CISPA seeks to have a decisive global impact on research, transfer and innovation.

CISPA addresses the entire range of subjects, from theory to empirical research. It is deeply grounded in computer science, with interdisciplinary links to the fields of medicine, mathematics and the social sciences. CISPA brings leading scientists in the field of cybersecurity and the aforementioned disciplines together. Its interdisciplinary approach establishes and shapes collaborations across existing thematic boundaries.

CISPA serves as a distinguished center of excellence for cybersecurity research and as an elite training ground for the next generation of scientific experts in this field.

### 3. Respect and diversity

Another important key to our success is treating each other with respect and fairness. We are prepared to learn from mistakes and appreciate frankness.

CISPA does not tolerate any form of discrimination, bullying or harassment in the working environment, no matter whether it is based on age, disability, origin, gender, political position or trade union activism, religion or sexual orientation.

#### **4. Equal opportunities**

Equal opportunities exist for all employees at CISPA. They all have the same opportunities, prerequisites and working conditions in terms of, for example, working hours or promotion prospects. With regard to the development of employees, the principal criteria are performance and potential.

At the same time, it is CISPA's declared objective to further entrench the principle of equality at the Center and, in particular, to encourage the breakdown of barriers in terms of genders in the field of IT.

#### **5. Safeguarding good scientific practice**

Scientific integrity is the basis of any trustworthy science. That is why CISPA takes its cue from the guidelines for the safeguarding of good scientific practice issued by the research association Deutsche Forschungsgemeinschaft (DFG).

Each employee engaged in scientific work must, in carrying out such work, adhere to the rules for safeguarding good scientific practice in order to avert any damage to science or to CISPA.

These rules play an important role in the training of young scientists and require special responsibility on the part of their supervisors.

#### **6. Technology transfer**

As a member of HGF, CISPA pursues long-term research and educational goals of the state and society.

Technology transfer takes place, above all, through transfer from head to head. CISPA aims to create, design and utilise innovative technologies for industry and for start-ups based on the results of its research and to make such results and technologies available on open source platforms. In doing so, CISPA sees itself as a driver and pioneer of disruptive technologies for the products and solutions of the future.

Developing Germany as a business location is of particular relevance. The establishment of a unique cybersecurity ecosystem, on the CISPA Innovation Campus too, will be a major long-term contribution towards achieving the goal of masterminding and facilitating structural change by means of large business hubs, start-up companies and added national value creation.

## **7. Promotion of young talent**

CISPA pursues the clear goal of becoming an international leader in cybersecurity research and a center of cybersecurity talent which is recognised worldwide. Therefore, it focuses not only on research itself but also on the promotion of young scientists.

## **8. Innovative, modern working**

CISPA uses all the options at its disposal to increase its attractiveness as an employer and provide its employees with an excellent work-life balance.

In particular, employees are offered a modern corporate culture, comprehensive further training opportunities and effective company health management, as well as flexible working hours, various part-time models and the chance to work remotely.

## **9. Corporate and social responsibility**

As a federal research organisation and publicly financed company, we are committed to our corporate and social responsibility. We bear this responsibility towards our employees, business and cooperation partners and sponsors likewise.

We ensure that the financial resources which are entrusted to us are treated responsibly, and we utilise them economically and sparingly.

## **10. Data protection**

We pay strict attention to compliance with the rules governing the protection of personal data. We protect confidential information and documents about CISPA, contractual partners or employees by treating them carefully and confidentially.

Personal data may only be processed (e.g. collected, stored, used) to the extent necessary and if a legal basis exists (e.g. consent is given). How their personal data is used must be transparent for the data subjects. Their rights to information and rectification and, where applicable, to objection, blocking and erasure or restriction must be safeguarded.

With regard to technological protection against unauthorised access to data and information, an adequate standard must be applied which is in accordance with the latest technology and, where possible, the latest science.

## **11. Export controls**

Due to the international nature of its research, CISPA is connected to a worldwide network of the most renowned researchers and prestigious cooperation partners. Within the scope of this intensive contact with foreign partners, adequate consideration must also be given to risks as far as export controls are concerned.

To prevent an uncontrolled circulation of weapons and misuse of sensitive research data, software or technologies, CISPA is obliged to comply with the relevant laws and regulations governing the export of goods, services and technologies and the transfer of know-how. Guests and other users of our infrastructure are also subject to these regulations.

## **12. Occupational safety, occupational medical care and occupational health management**

Occupational health and safety take top priority at CISPA. Every employee has a right to a safe and healthy working environment and contributes to this with their own responsible behaviour.

In the course of setting up the new center, the required occupational health management measures will be integrated into all operational processes. This has the aim of maintaining and promoting the health, motivation and well-being of all employees.

## **13. Avoiding conflicts of interest and combatting corruption**

When employees get into a conflict between their personal interests and their professional tasks or the interests of CISPA, this can damage CISPA's reputation. Therefore, corrupt behaviour is not tolerated at CISPA. As a rule, even any appearance of being susceptible to personal benefits within the scope of the employment relationship must be avoided.

Corruption can be better prevented if everyone is committed to the goal of fighting corruption. Appropriate measures should be taken in terms of personnel, organisation and administration to prevent any misappropriation of funds and to prevent business operations from being affected by corruption.

## **14. Protection of corporate property**

As a research organisation, we make the protection of CISPA's corporate property a core element of our business policy.

CISPA's property encompasses not only tangible assets but also intangible assets such as industrial property rights, copyrights and other rights to intangible assets.

Each and every employee shares responsibility for protecting these corporate values. Therefore, everyone is expected to treat CISPA's property with the utmost care and use it only for its intended purpose.

## **15. Complaints and reports**

Every employee can submit a complaint to their supervisor, the HR department, the works council or another body designated for this.

Circumstances suggesting a breach of the Code of Conduct can be reported to the Internal Audit and Compliance department or via the whistleblower system.

## **16. Coming into effect**

This Code of Conduct enters into force on 1st April 2024.

Saarbrücken, 1st April 2024