ATHENE
National Research Center
for Applied Cybersecurity

Research and Knowledge Security

A Risk- and Opportunity-Based Approach for ATHENE
and its Participating Organizations – Best Practice

ATHENE — National Research Center for Applied Cybersecurity

Executive summary

Open, internationally connected research is a source of strength for Germany and for ATHENE. The same openness can be exploited: through espionage, the leakage of dual-use knowledge, cyberattacks, undue influence, and damage to reputation. This document sets out a best practice for protecting research and people without sacrificing the openness on which innovation and progress depend — offered by ATHENE for its participating organizations to adopt and for peers to borrow.

The practice rests on one idea: **weighing risks against chances**, case by case. It is deliberately neither laissez-faire nor closure. Every decision (whom to hire, with whom to cooperate, what to publish, what to export) runs through a single, proportionate process that asks what is at stake, what the risk is, what the scientific opportunity is, and what response is proportionate. "Risk management" here does not mean certification against a standard; it means staying continuously aware of the risks and the opportunities of a decision.

ATHENE is a research center of the Fraunhofer-Gesellschaft, with its two institutes Fraunhofer SIT and Fraunhofer IGD and with the involvement of TU Darmstadt, Goethe University Frankfurt, and Darmstadt University of Applied Sciences. ATHENE is not an independent or joint legal entity; it does not sign contracts, hire people, or run projects. Doing so is the sole responsibility of the participating organizations. ATHENE, as a center, never carries the responsibility for research security. What ATHENE does is **define this common practice and encourage everyone to apply it**, and offer shared instruments — an advisory Research Review Board, a maintained partner-tier list, a situational picture of the cyber threat — that make adoption easier. For the work it funds, ATHENE adds one light expectation: **that the recipient apply this practice, or an equivalent process, and confirm on request that it was done** — which is how ATHENE discharges its own organizational responsibility for its funding. Beyond the funding ATHENE itself provides, it does not enforce or audit, and there is no inspectorate; adoption is professional good practice, not obligation.

In short, the best practice rests on: a **single decision method** (Section 2) with three risk tiers and a partner-tier logic; a **model of graduated responsibility** (Section 3) under which each participating organization runs research security through its own organs, supported by a thin shared layer; **seven pillars** (Section 4); and a **minimal, cost-reasonable apparatus** (Section 5) whose effectiveness each adopter can measure.

Contents

1 Scope and principles

1.1 Scope

This best practice covers research and development, teaching and consulting, as well as science management across ATHENE and its participating organizations, and addresses six things that can be put at risk: **personnel**, **partnerships**, **IT and research data**, **intellectual property**, **exportable technology and knowledge**, and the **ethical integrity** of the work. "Partnership" includes all persons and organizations with which ATHENE cooperates or does business, or which provide funding to or receive funding from ATHENE. The work itself is carried out by the participating organizations, which hold the legal responsibility throughout — including for the activities the ATHENE office runs, where the responsibility rests with the participating organization through which the office acts. The single decision method that runs through all of it is set out in Section 2; Section 3 sets out who does what.

Two duties are not a matter of choice: they bind every participating organization as a legal entity, whether or not it adopts this practice. **Export-control law** (the German Außenwirtschaftsgesetz and -verordnung and EU Regulation 2021/821) and **EU and national sanctions** are mandatory, and data-protection law applies to any screening. "Voluntary" in this document (Section 3) describes the recommended practice ATHENE adds *on top of* that legal floor — not the floor itself, which the export-control and personnel pillars (Section 4) restate.

1.2 Principles

The practice rests on a small set of principles that hold even when they pull in different directions.

Openness is the default.
Restriction is the exception that must be justified, not the starting point. The burden of argument is on closing down, not on staying open.

Academic freedom carries great weight, but is not absolute.
Freedom of research and teaching is guaranteed by Art. 5(3) of the Basic Law (Grundgesetz) without an explicit statutory reservation, and it weighs heavily. It is not unlimited: it may be restricted to protect competing rights or goods of constitutional rank, and then only by proportionate means. Security measures here do not override it lightly; they must serve such a competing good and pass the proportionality test below. This is the constitutional ground on which export control and dual-use limits stand, while a blanket restriction would not.

Proportionality.
The depth of any check scales with the actual risk. Low-risk activity stays light-touch; scrutiny is spent where it changes the outcome.

Risk against chance, case by case.
Decisions weigh the specific risk against the specific scientific opportunity. There are no blanket bans and no blanket clearances (Section 2).

Graduated, shared responsibility.
Responsibility is shared across the researcher, the project, the institution, and the center; each level does what it is best placed to do.

Alignment with declared positions.
The practice is consistent with German and European science-policy positions toward partners, set out most recently in the German federal and European research-security framework [2, 4], as operationalized in this document: close cooperation within trusted circles such as the EU and NATO and among like-minded countries; differentiated cooperation, including competition, with systemic rivals such as China [14]; and no cooperation that sanctions or embargoes forbid. These stances enter the method as *partner tiers* (Section 2), which steer the level of scrutiny; they are not a static blacklist, and only a legal prohibition (sanctions, embargo) makes cooperation a settled "no."

Fair process for the individual.
Because some measures fall on individuals, the practice builds in safeguards: a documented basis for any restriction, assessment on role and conduct rather than origin, data minimization, a route to have a decision reviewed, and a default that restrictions lapse when their reason does. Equal treatment before the law (Art. 3 of the Basic Law) and the General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz, AGG) point the same way, even though neither addresses nationality explicitly.

2 The risk-and-chance method

Every pillar in this practice reuses one decision process, so that a project leader learns it once and applies it everywhere. The process echoes the generic risk-management cycle of ISO 31000 [16] and makes one step explicit and central that policy debates tend to drop: a deliberate weighing of the scientific *opportunity* against the risk, so that protection is never decided in isolation from what would be lost by saying no. None of this is new in kind: weighing openness against protection, proportionately and case by case, is the settled consensus of research-security policy — resting on the constitutional proportionality test, the ISO 31000 risk cycle, the EU's principle of staying as open as possible and as closed as necessary [6] and the "de-risking, not de-coupling" of current China policy, and the case-by-case guidelines of the Max Planck Society, the DFG and Leopoldina, and the Wissenschaftsrat [12, 18, 26]. This practice's contribution is synthesis and operationalization across the seven pillars, not a new principle.

1. **Identify the asset and the stakes.** What knowledge, data, technology, person, or relationship is involved, and what would be lost if it were compromised?
2. **Assess the risk.** Consider the partner, the person, the country, and the technology together. Use risk *indicators*, not blacklists: the human-rights and academic-freedom situation, corruption and democracy indices, sanctions and export-control status, and any history of espionage or coercion [18].
3. **Weigh the chance.** State the scientific and strategic opportunity the activity offers. A significant opportunity can justify accepting and managing a higher risk; a marginal one cannot.
4. **Choose a proportionate response.** One of: proceed; proceed with safeguards; escalate for a higher-level decision; or decline. Declining is the last resort, reserved for risks that cannot be brought to an acceptable level.
5. **Record, monitor, review.** Document the decision and its reasons, monitor whether the safeguards actually work, and revisit the decision as circumstances change.

Risk tiers. Activities fall into three tiers, and the tier sets who decides and how much scrutiny applies. A single trigger is enough to lift an activity to the higher tier.

Low.
The default for routine, open, fundamental research with partners in the trusted circle. The researcher documents a short self-assessment and proceeds.

Elevated.
Any of: a dual-use-adjacent topic; a partner in a high-risk tier, or a person with a current or recent affiliation to an institution in a high-risk tier *where the role gives access to sensitive assets* (the trigger is the affiliation-plus-access, never nationality); access to sensitive, non-public research data; or external funding that carries conditions or reputational concerns. The project leader decides, with input from the relevant specialist function (export control, data protection, ethics).

High.
Any of: the work requires export classification or licensing, or gives access to controlled technical detail; the partner is in the embargoed/sanctioned tier or on a named organization of concern; the activity is a security-sensitive project; or there is a credible, specific adverse indicator on a person or partner. In the recommended model the decision rises to the leadership of the participating organization that runs the work, with the Research Review Board advising where ethics is in play. To keep this from becoming a bottleneck, leadership can delegate routine high-risk classes to a standing committee, and every tier carries a target turnaround time so that scrutiny does not stall the science.

The point of the tiers is to spend scrutiny where it changes the outcome and to leave ordinary science unburdened. The default posture, when risk and opportunity are both real, is to *proceed with safeguards* rather than decline. But an institution should be prepared to decline, or walk away from, a cooperation whose residual risk cannot be brought to an acceptable level — and for its own activities ATHENE holds itself to the same.

Watch the aggregate, not just the case. The tiers above weigh one decision at a time, and each of the individual red flags — a defense-linked partner, foreign-state funding with strings, access to controlled detail — already lifts its own case on its own. What single-case review cannot see is *accumulation*: a group can clear every case on its merits — each hire proportionate, each grant individually acceptable, each data-access scoped — and still end up, over time, with most of its sensitive work, its funding, and its access to the same crown jewels resting on a single external state. No one decision was wrong; the concentration is the exposure. So the practice adds a periodic look at the group or project as a whole, which can raise its posture even when no individual case would. The measure is the *share and density* of affiliations, funding, and access — never nationality, and never a count of how many people come from any one country. Throughout, scrutiny attaches to affiliation and access, not to a person's nationality or origin: the equal-treatment principle of Section 1.2 governs, and the only categorical "no" comes from a binding legal prohibition — a sanction or an embargo — never from where a person is from.

Security-sensitive projects. Because ATHENE is a cybersecurity center, almost all of its work is *about* security; that alone does not make a project security-sensitive. What matters is not the topic but the misuse potential of the specific output: a project is **security-sensitive** when the knowledge, data, or tools it produces would cause concrete harm if they leaked or reached the wrong hands. In practice this covers work that develops offensive capabilities or working exploits for undisclosed vulnerabilities (zero-days), or attack tooling usable against systems in the field; work whose results could enable attacks on critical

infrastructure; classified, export-controlled, or contractually confidential work; the handling of sensitive non-public data (real vulnerability details of named operators, incident data, or personal data); and dual-use-of-concern results that would materially lower the cost or raise the impact of attacks. Open, defensive, publishable fundamental research is *not* security-sensitive. Sensitivity is the exception, decided case by case on the specific output and the access it requires; it is what lifts a project to the high-risk tier and may attract the access conditions of Section 3.

Partner tiers. Orthogonal to risk tiers, partners are grouped by the declared positions in Section 1.2: **trusted circle** (e.g., the EU, NATO, and other like-minded countries such as Australia, Israel, Japan, New Zealand, and South Korea); **systemic rivals** (differentiated cooperation and competition, e.g., China); **high-risk** (heightened scrutiny and case-by-case decision); and **embargoed or sanctioned** (cooperation prohibited to the extent that sanctions, embargoes, or export controls reach it). The two ends differ in kind: a *high-risk* partner raises the tier and triggers safeguards or escalation, but is decided case by case; with an *embargoed or sanctioned* partner, cooperation is a legal "no" wherever the binding restriction applies. To make the tiers operable, the Chief Research Security Officer (Section 3) maintains a **living ATHENE partner list** of countries and organizations mapped to these tiers — held as the partner-tier table, the named-organization watch sources, and the indicator sources in the living appendix (a separate, regularly-updated companion document). The list is built from criteria — sanctions and embargo status, named-organization lists (e.g., the EU), and human-rights, academic-freedom, corruption, and democracy indicators — and is reviewed on a fixed cycle so it does not ossify into an outdated blacklist. It sets the *starting* tier for scrutiny; except for the embargoed/sanctioned tier, it never substitutes for the case-by-case judgment of this method. Because such a list is the most sensitive instrument in this practice, its governance is fixed: the CRSO owns it; its sources and update cycle are documented; changes are logged; a partner may ask for a tier to be reviewed; and a country tier is evidence about a *place*, not a verdict about a *person*. It may raise the scrutiny of an activity, but it reaches an individual only through the role-and-access test of the elevated tier above.

Worked example. A doctoral candidate from an institution in a high-risk country applies for a position in an ATHENE-funded project on a topic adjacent to a controlled technology. *Step 1* — the asset is the project's know-how and any controlled technical detail the role would give access to; the stake is leakage to a foreign end-user. *Step 2* — the risk is elevated: the home institution sits in a high-risk tier and the topic is dual-use-adjacent, though there is no specific adverse indicator on the individual. *Step 3* — the chance is real: the candidate is strong and the line of work valuable. *Step 4*, proportionate response — proceed with safeguards rather than decline: the candidate is hired into the open part of the project; access to the controlled detail is scoped and, if needed, deferred until an export-control check clears it; the supervisor and the export-control function sign off, and declining is reserved for the case where the controlled core cannot be separated from the role. *Step 5* — the decision, its reasons, and the access scope are recorded, and the arrangement is reviewed if the project or role changes; the assessment turns on role, access, and topic, not on nationality. ATHENE does not step into the hiring here: the participating organization runs the vetting and scopes the access as part of its own responsibility for research security — exactly the good practice this document recommends; ATHENE's part is to have articulated the practice and to make the shared instruments available (the Research Review Board, the partner-tier list), not to direct the organization's internal process.

3 Governance and roles

3.1 How the best practice works

ATHENE is a center of the Fraunhofer-Gesellschaft and a consortium of five participating organizations in four legal entities, and the cooperation agreement [11] sets out how it works. Each participating organization that hires staff or runs a project does so under its own responsibility and through its own processes: it vets the people it employs, screens sanctions lists, classifies exports, and decides on publication. Research security is its responsibility, in every case. This document describes the practice recommended by ATHENE for these processes, and ATHENE encourages every participating organization — and peers beyond ATHENE — to adopt it. ATHENE states the common standard, points to the competent function, and offers shared instruments. Beyond a single light expectation attached to the work it funds (below), it does not require adoption or audit it. The aim is that good practice spreads and that no risk falls through the gaps between the participating organizations, not that ATHENE builds an inspectorate over institutions that answer to their own law.

Activity	**Who performs it (and is responsible)**	**What ATHENE offers**
Hiring a person	The participating organization that hires: vetting, sanctions screening, employment	Recommends the practice; offers the Research Review Board and the partner-tier list
Running a project	The participating organization that runs it	Recommends the method and its documentation; points to that organization's functions
Export classification & licensing	The participating organization's export-control function	Recommends that controlled work reach that function early
Publication decision	The participating organization, via the cooperation agreement's procedure	Recommends the last-resort review route; the shared Research Review Board advises on request
Cybersecurity of IT and data	The participating organization's IT / information-security function	Recommended baseline, shared situational awareness, incident coordination
Work of the ATHENE office	The participating organization through which the office acts	The office applies the same practice to its own activities

Table 1: *Roles and responsibilities.* Who performs and is responsible for each activity, and what ATHENE offers as shared good practice. For the work it funds, ATHENE also asks that the practice (or an equivalent) be applied and confirmed on request.

3.2 The legal map: who holds the statutory duties

The cooperation rests on a cooperation agreement and the ATHENE rules of procedure [8, 11], and ATHENE has no legal personality of its own. Because it is not a legal entity, the statutory duties sit with the participating organization: export-control liability, employment decisions, and the role of data-protection controller under the GDPR belong to the participating organization that employs the person or runs the export, not to ATHENE as a center.

For data protection this is not built from scratch: the participating organizations operate a joint-controllership agreement under Art. 26 GDPR under which the Fraunhofer-Gesellschaft is the central contact point for data subjects, impact assessments are conducted jointly, and a common data-breach process applies [21]; the agreement binds the founding entities, and Goethe-Universität is covered through its 2022 accession [10]. Whether a given research-security screening falls under that agreement is decided per processing activity: where it does, the agreement is used; otherwise the responsible participating organization establishes the controller role, legal basis, notice, and retention before any personal data is processed. Personal data used for a check is limited to what the check needs, with a documented legal basis and a defined retention period (Annex 6.5).

3.3 The common standard, and how it spreads

ATHENE does not build a second bureaucracy on top of the participating organization. The model is **a common standard carried by subsidiarity**, resting on three commitments. First, the practice is **complete on its own terms**: it states the objectives, expectations, and recommended minimum in full, so a reader sees the whole practice without consulting four participating-organization regimes. Second, **execution stays with the participating organization's own organs**, which hold the competence and the legal duty. Third, ATHENE **commends the standard and helps adoption**: it offers the shared instruments, shares lessons, and — on request — will review and acknowledge a participating organization's practice against the standard. Adoption is voluntary good practice, with one bounded exception: **for the work ATHENE funds**, ATHENE asks the recipient to apply this practice (or an equivalent process) and to confirm, on request, that the competent process was run. That single funding-linked expectation is how ATHENE discharges its own organizational responsibility for the money it gives; its only remedy, in the last resort, is to decline to fund. Beyond the funding ATHENE itself provides, it recommends but does not require. Where a participating organization has no suitable organ, ATHENE offers the Research Review Board (Section 3.5) rather than improvising a check of its own.

The confirmation clause. ATHENE implements this expectation as a single clause in the award or forwarding agreement (Zuwendungsweiterleitungsvertrag): *"The recipient applies the ATHENE Research and Knowledge Security best practice, or an equivalent process of its own, to the funded work, and confirms on request that the competent process was run. ATHENE does not re-perform the check."* The clause records that the recipient's own competent process ran; it is a confirmation, not an ATHENE audit of the result, and adds no second layer of approval.

For its **own security-sensitive projects and partnerships** — meaning the work ATHENE funds or that carries the ATHENE name —, ATHENE may ask for measures beyond the recommended baseline — for example scoped or deferred access to controlled detail, or extra documentation of prior affiliations for a sensitive role. Because the work is run by a participating organization, ATHENE asks; the participating organization, as the responsible party, decides and implements. ATHENE is a civilian center and cannot grant a statutory security clearance; "access conditions" means project- and role-specific restrictions that the participating organization applies. For the activities the office runs itself, the office follows the same practice.

3.4 Decision levels and the shared apparatus

The recommended model places each decision at the lowest level competent to take it: the **researcher** self-assesses routine work; the **project leader** decides elevated-risk cases with specialist input; the **participating organization's leadership** decides high-risk cases; and the **Research Review Board** advises on security-relevant research. A small shared apparatus, offered by ATHENE, supports this:

- A **Chief Research Security Officer (CRSO)** at ATHENE level: a single named function that curates the practice, maintains the checklist and the living partner list (Section 2), is the point of contact, convenes the Research Review Board, shares lessons across the participating organizations. The CRSO is nominated by the ATHENE CEO and appointed by the ATHENE Board.
- The participating organizations' **export-control and compliance functions**, which run sanctions-list screening and export classification for their own legal entity.
- The **ATHENE Research Review Board (RRB)**, for the ethical and research-security questions of ATHENE research, available to participating organizations without their own ethics organ. It follows the DFG/Leopoldina framework [12] (defined in Section 3.5).

The apparatus is light enough for every participating organization to work with and complete enough that the practice's objectives are met regardless of which participating organization hosts the work. ATHENE offers it; each participating organization uses as much of it as it needs.

3.5 The ATHENE Research Review Board (RRB)

Besides the CRSO, the **Research Review Board (RRB)** is the one standing body this practice sets up. It is an advisory board that any ATHENE principal investigator or project can call on for the ethical and research-security questions a piece of work raises — dual-use and misuse potential, research ethics and the handling of sensitive or personal data, security-sensitive output and coordinated disclosure, and the publication-restriction question of last resort. It does not replace a participating organization's own organs; it complements them and serves those that have none.

The board *follows* the DFG/Leopoldina framework for the ethics of security-relevant research [12] as its model of good practice. It is deliberately *not* a Committee for the Ethics of Security-Relevant Research (KEF) in the formal sense: ATHENE has no senate or the institutional organs a statutory KEF presupposes, and the board issues *non-binding advice*, not binding decisions. Where a participating organization has its own KEF, that KEF governs; the RRB is the shared, ATHENE-level body for those that do not, and a voluntary second opinion for those that want one.

What it does. The RRB works in two modes:

- **Formal review.** On request it issues a reasoned, written, non-binding opinion on whether a piece of security-relevant or dual-use research should proceed, proceed with conditions, or be reconsidered — normally within four weeks, sooner where a matter is urgent.
- **Early consultation.** A low-threshold channel where researchers can talk a case through *before* they are committed. This is the board's most useful function in practice: it shapes a project while choices are still open rather than judging it at the end.

It is also the route by which the last-resort publication review of the openness principle

(Section 4) reaches an independent opinion, and it curates a short code of conduct for security-relevant research and guidance on coordinated ("responsible") disclosure.

Its charter (Satzung). The board works from a short charter, maintained by the ATHENE Board, that defines: its remit (the research-security aspects of ATHENE research, with the ethics of security-relevant and dual-use research at its core); its advisory role (it advises and does not decide — the decision stays with the participating organization that runs the work); its referral and record-keeping procedure; its handling of conflicts of interest and confidentiality; and its adherence to the DFG/Leopoldina framework [12].

Membership. The board has between five and seven members and elects its own chair from among its members, combining research-ethics, legal and export-control, data-protection, and security expertise. The members are nominated by the ATHENE CEO and appointed by the ATHENE Board for three-year terms; members serve in a personal capacity, not as delegates of their institution.

3.6 Decision rights, conflicts, and adoption

Who signs off. In the recommended model each risk tier has a named decision owner (Annex 6.3), sitting inside the participating organization that runs the work. The CRSO curates the practice and offers support but does not approve projects or sign off on a participating organization's decisions.

Where judgments differ. Because research security is the participating organization's responsibility, the participating organization's judgment governs its own work; ATHENE neither compels a participating organization to proceed nor overrides its refusal. For ATHENE's own activities, a negative or stricter judgment by either the legally competent participating organization or by ATHENE stops the *ATHENE* activity until it is resolved. Where a restriction would touch employment or access, the participating organization's legal review governs how it is implemented.

Adoption, with a light touch on funded work. ATHENE runs no inspectorate and audits no one. Its assurance that the practice works is mostly indirect and voluntary: it shares the standard, the checklist, and the shared instruments; it offers, on request, to review and acknowledge a participating organization's own process; and it learns from the cases that come to the Research Review Board. The one firmer point is the funding-linked expectation of Section 3: for the work it funds, ATHENE asks the recipient to confirm, on request, that the competent process was run, and keeps that confirmation — not to re-perform the check, but to discharge its own responsibility for its funding. A participating organization that adopts the practice does so as good professional practice and keeps its own record; what it shares with the CRSO feeds the effectiveness measures of Section 5. For its own activities, ATHENE holds itself to the same practice it recommends.

Brand and funding. ATHENE cannot override a participating organization's legal right to proceed with a project its own competent bodies have cleared. It can, however, decline to be associated with that project. ATHENE reserves the right to withdraw its funding, and to withhold the use of the ATHENE name and affiliation, from any activity whose residual risk exceeds what the center is willing to stand behind — even where the participating organization has cleared it. This is not a veto over the work; it is ATHENE's control over its own money and its own name.

Raising a concern. Anyone involved in ATHENE-related work can raise a research-security concern in confidence — a suspicious approach, an attempt at coercion, or a decision they believe understates a real risk — without going through the person whose decision is in

question. The ordinary route is to the CRSO. Where the concern involves the CRSO, it may be raised instead with any of the CEO, the COO, or the chair of the Research Review Board. A concern raised in good faith carries no disadvantage for the person who raises it.

4 The pillars

Each pillar states a short rule, the triggers that raise a case above routine, and where execution sits. All pillars share the method of Section 2. The rules are written as the practice itself: each states what good research security requires and is carried out by the participating organization that runs the work. ATHENE's part is to recommend the rule and offer the shared instruments — and to follow the rule for its own activities — not to perform the check itself.

4.1 Cybersecurity

Rule. Protect the confidentiality, integrity, and availability of the IT and data of research, teaching, and administration in proportion to their value and exposure, and be able to detect and recover from incidents.

This is the pillar where ATHENE conducts its own research: its situational picture of the attack surface of German research institutions — the ATHENE Lagebild [19] — feeds both the national debate and ATHENE's own posture.

The baseline. The recommended cyber baseline puts the order first: know and clean the infrastructure, then harden the architecture, and only then add governance on top — ATHENE expects it for the research it funds and encourages it everywhere else. In sequence that means a complete inventory of systems and of the external attack surface (what is not known cannot be protected); decommissioning of end-of-life systems and consolidation of decentralized IT; automated patch and configuration management; a zero-trust architecture with segmentation, multi-factor authentication, least privilege, and no default credentials; monitoring with the ability to detect and recover, backups included; and an information-security function with real authority — full-time, with a genuine veto. The architecture must also be able to separate research by sensitivity: the most sensitive data, systems, and projects are isolated in their own segment with their own access controls, so that a compromise elsewhere does not reach them. A management system and certification come after this base is in place, not instead of it: compliance laid over an unpatched, uninventoried estate adds cost without adding security.

Triggers and execution. Sensitive or personal research data and systems that support critical processes raise a case above routine, as does any system within the scope of the German NIS-2 regime — the BSIG as amended by the NIS-2 implementation act [3], in force since December 2025. That regime is narrow, however: it reaches only research organizations whose *primary* purpose is commercial applied research, above the size thresholds. Among ATHENE's members it captures the Fraunhofer institutes; universities are excluded as educational institutions, most non-university research is out of scope, and the Länder have additionally exempted their own universities from the transposition. Day-to-day operation sits with the participating organization's IT and information-security functions; ATHENE's contribution is a recommended baseline, shared situational awareness, and incident coordination. Participating organizations are encouraged to share with the CRSO any incident that materially affects shared or ATHENE-related research or data — alongside, not in place of, their own statutory reporting — so that the situational picture stays current.

Travel and mobile access. Sensitivity travels with the researcher. For travel to high-risk or systemic-rival destinations, the recommended baseline is clean loaner devices carrying only what the trip needs, full-disk encryption, and temporary suspension of access to the most sensitive systems for the duration, restored on return. The measure attaches to the destination's risk and the data carried, never to the traveler.

4.2 Personnel vetting

Rule. Check the people brought into sensitive work to a degree proportionate to the sensitivity, within the limits of law and non-discrimination.

The pillar covers visiting researchers, doctoral candidates, and guest scientists as well as regular hires. The baseline check is sanctions-list screening, run in each participating organization's export-control or compliance function. Above the baseline, for its own security-sensitive projects and partnerships ATHENE may ask for additional *access conditions*, which the hiring participating organization — as the responsible party — decides on and implements (Section 3). These conditions are tied to the role and the topic, never to nationality, and are drawn from a fixed menu:

- **Scoped or deferred access** to controlled technical detail until an export-control check clears it.
- **Documentation of prior affiliations** for roles that touch controlled work.
- **A named-organization affiliation check** — in the manner of Canada's Named Research Organizations list [13], or, more broadly, an affiliation-disclosure and due-diligence check in the spirit of Australia's UFIT framework [22] — available as an option for high-risk roles, not a blanket requirement. Among the participating organizations, TU Darmstadt runs such an internal screening process for guest researchers funded by foreign government scholarship programs.

Two limits are part of the rule, not exceptions to it. Checks are **proportionate and non-discriminatory**: nationality is not a proxy for risk, and a person is assessed on role, access, and concrete indicators, not on origin. And checks respect **data-protection law**: only data necessary for the specific assessment is processed, and the basis and retention are documented. ATHENE is a civilian center, and its personnel measures stay within what civilian employment and data-protection law allow.

4.3 Partnership and cooperation vetting

Rule. Before and during a cooperation, run due diligence on the partner proportionate to the partner tier and the topic.

The reference models are closest to home: the Fraunhofer cooperation-compliance guidance [9] which sets objective partner-selection criteria and binding compliance steps such as sanctions-list screening and central export-control review, and the HRK standards for international cooperation [15], which call for robust governance, risk analysis, and exit strategies in international partnerships. The most detailed instrument is the consolidated guideline of the Max Planck Society [18], which pairs a case-by-case, topic- and country-specific assessment with a concrete checklist of contract clauses: sanctions-list screening, due diligence on a partner's ownership and financing, export-control clauses, and clauses on intellectual property and IT security. ATHENE adopts the same shape. The DAAD's KIWi-Checkliste Wissenssicherheit [5] is the closest German counterpart to this practice's own decision checklist.

Red-flag indicators — opaque ownership, links to a foreign military end-user, a partner in a high-risk tier, or pressure to restrict publication — raise a case to elevated or high risk. For cooperation with partners in the People's Republic of China, the practice follows the HRK's differentiated, values-based approach rather than either decoupling or unconditional engagement [14, 15]; this "de-risking, not decoupling" posture is the one carried forward by the current German federal and EU research-security framework [2, 4].

Among these red flags, *military-civil fusion* is worth naming explicitly: in systemic-rival states a nominally civilian university or firm can be bound into the defense apparatus, so a civilian counterpart is not, on its own, reassurance. This indicator is about a partner's entanglement with a foreign military-industrial complex, not about defense research as such — cooperation with the German Bundeswehr and with allied armed forces is a legitimate and wanted part of ATHENE's work and runs through the ordinary method, not through this red flag. For the People's Republic of China, the ASPI China Defence Universities Tracker [17] is a useful starting indicator, read as evidence about an *institution*'s entanglement.

4.4 Export control

Rule. Comply with export-control law, and treat the academic exemptions as real but narrow.

Export control reaches research because the controlled object is not only equipment but "technology" — knowledge itself. Under EU Regulation 2021/821, controlled technology includes intangible transfer: sending software or technical detail abroad by email — or reading out a controlling technical document over a phone call — can make a researcher the exporter who needs a license [7]. EU export law exempts open science only narrowly: the carve-out for "basic scientific research" is narrow, and applied work must instead qualify as being "in the public domain." The exemption is narrow and defeasible. It covers information, not controlled items; it lapses once a sponsor attaches a publication restriction; and it is overridden by catch-all controls and by sanctioned end-users. Germany's BAFA puts the point plainly for researchers: academic freedom is no "Freifahrtschein" that suspends export-control law [1].

Execution. Classification, licensing, and the role of the export officer sit with each participating organization's export-control function, where the legal liability already lies. ATHENE's contribution is to make sure every project that touches controlled technology reaches that function early, through the trigger in Section 2.

Remark: the US export-control regime. The export-control law binding on a German center is the German and EU regime above. The US regime — the EAR's deemed-export rule, the Fundamental Research Exclusion, OFAC sanctions, and the Entity List [23, 25] — is *not* binding German law and on its own creates no German licensing duty. It is still worth keeping in view, because it can reach ATHENE's work in practice: research software and equipment is often US-origin and stays subject to the EAR; giving a foreign person access to US-controlled technology can itself be a controlled release — a *deemed export* inside the United States, or a *deemed reexport* where US-origin technology already abroad is released to a national of a third country; and US sanctions and Entity-List restrictions reach US-origin items, US persons, and US-dollar transactions in a collaboration. These are considerations to weigh in the case-by-case method, not obligations under German law.

4.5 Intellectual property and knowledge protection

Rule. Identify the knowledge worth protecting and protect it by the least restrictive means that works.

Not all knowledge needs protection; the pillar starts by naming the few "crown jewels" (the methods, datasets, or results whose loss would do real harm) and concentrates protection there. The ordinary instruments are largely already in place. ATHENE does not invent an intellectual-property regime: ownership of work results, the handling of inventions and inventor compensation, joint patent filing, and the allocation of copyright and usage rights follow the existing cooperation agreement (its work-results clause, §5), which rests on German employee-invention law *ArbNErfG* [11]. Confidentiality is likewise covered by the agreement's confidentiality clause; this practice adds only the research-security overlay: deciding *which* crown jewels warrant protection beyond the contractual default, and pairing that with IT-security clauses where a cooperation touches them.

Restricting or delaying publication is a last resort, used only when a specific, serious risk cannot be managed any other way; the participating organization decides on the Research Review Board's advice, any restriction is time-limited, and it is never a routine default. The openness principle of Section 1.2 applies here with full force. In practice it operates through the existing cooperation agreement's publication procedure (§7), under which a participating organization publishes its own results freely and jointly-produced results are coordinated among the participating organizations within a fixed review window [11]; the research-security last resort is the rare case that procedure escalates to the Research Review Board, not a parallel clearance step.

4.6 Research ethics and responsibility

Rule. Manage the dual-use and misuse risks of the research through self-regulation, without disproportionately restricting the freedom of research.

The German science community has run a self-regulation framework for security-relevant research since 2014, updated in 2022, jointly issued by the DFG and the Leopoldina [12]. It treats scientific freedom and scientific responsibility as two sides of one coin: researchers carry out a risk analysis, minimize and document risks, review whether a result should be published, and, in the last resort, forgo a line of work; institutions support them through ethics rules and a KEF. ATHENE adopts this framework and makes the Research Review Board (Section 3.5) the route to such an opinion for participating organizations that lack their own — or want a second opinion. The dual-use frontier is moving: AI systems built for beneficial science can be repurposed for harm, as when a drug-discovery model was redirected to generate tens of thousands of toxic molecules [20, 24]. The aim is to catch the rare dual-use-of-concern case early, not to subject ordinary research to ethics review.

4.7 Keeping the practice current

Rule. The practice is reviewed, communicated, and measured, so that it stays in use rather than on a shelf.

The CRSO runs a regular review cycle, short training for project leaders, and a small set of effectiveness measures (Section 5). The practice is revised when the threat picture, the law, or ATHENE's partnerships change.

5 Footprint and effectiveness

The footprint is deliberately small: the CRSO function, the checklist and triggers of Section 2, the participating organizations' export-control and compliance functions, and the Research Review Board. No new approval body sits between a researcher and routine open science.

Each adopter can watch effectiveness with a few simple measures: the share of projects that completed a documented risk check, the time a check takes, the number of cases escalated and how they were resolved, and whether any safeguard failed in practice. These numbers show whether protection is proportionate or has drifted toward either neglect or over-control, and — where a participating organization chooses to share them — they make the practice's effect visible to peers who adopt it. The CRSO keeps them in the effectiveness dashboard of the living appendix, with the maintenance and change log.

6 Operational annexes

6.1 Decision checklist

For any new project, hire, cooperation, or publication that is not plainly routine, the responsible person answers:

1. What asset is involved, and what would be lost if it were compromised?
2. Who is the partner, person, or country, and what tier are they in?
3. Does the topic touch controlled or dual-use technology?
4. What is the scientific opportunity, and how large is it?
5. What is the resulting risk tier (low / elevated / high)?
6. What response is proportionate (proceed / safeguards / escalate / decline), and which safeguards?
7. Who must sign off, and which specialist function must be involved (export control, data protection, ethics)?
8. Where is the decision recorded, and when is it reviewed?

6.2 Decision record

One short record per non-routine decision: date and author; activity and asset; partner/person and tier; risk tier and the reasons; opportunity; response and safeguards; sign-off and specialist input; review date. The record is the audit trail and the basis for the effectiveness measures.

6.3 Escalation and sign-off matrix

In the recommended model the participating organization keeps these records; the CRSO curates the shared template and does not approve projects.

6.4 Routing and contact register

The populated routing and contact register — which office and function in each participating organization holds each statutory duty (export control, ethics, data protection, information

Risk tier	Decides	Specialist input	Documentation
Low	Researcher	— (self-assessment)	Short self-assessment note
Elevated	Project leader	Export control / data protection / ethics, as relevant	Decision record (Annex 6.2)
High	The participating organization's leadership	Export-control function; Research Review Board where ethics is in play	Decision record + sign-off

Table 2: *Escalation and sign-off.* By risk tier (recommended model; the owners sit inside the participating organization that runs the work).

security) — is the *routing register* in the living appendix. ATHENE sets out the standard and coordinates; each participating organization carries the statutory duty and the responsibility. Named individual contacts are held in the CRSO's working copy.

6.5 Data and retention

Any personal data used for a check is limited to what the check needs, with a documented legal basis and a defined retention period. The data-protection roles are decided per processing activity, as in the legal map (Section 3): where the screening falls under ATHENE's Art. 26 GDPR joint-controllership agreement [21], the participating organizations are joint controllers, the Fraunhofer-Gesellschaft is the central contact point for data-subject requests, impact assessments are run jointly, and the agreement's data-breach process applies; otherwise the responsible participating organization is the sole controller for that activity. Retention follows the retention schedule of the participating organization that processes the data; in the absence of a more specific schedule, decision records and sanctions-screening results are kept for the statutory audit period and then erased. Concrete retention classes are set per participating organization.

References

[1] Bundesamt für Wirtschaft und Ausfuhrkontrolle. Exportkontrolle und Academia: Handreichung für die Wissenschaft. Handreichung, BAFA, 2025. URL https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_aca_handreichung_wissenschaft.pdf.

[2] Bundesministerium für Forschung, Technologie und Raumfahrt. Eckpunkte zur Stärkung der Forschungssicherheit und zum Aufbau einer Nationalen Plattform für Forschungssicherheit. Eckpunktepapier, BMFTR, December 2025. URL https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2025/25-eckpunkte-forschungssicherheit.pdf.

[3] Bundesrepublik Deutschland. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG). Gesetz BGBl. 2025 I Nr. 301, Bundesgesetzblatt, December 2025. URL https://www.recht.bund.de/bgbl/1/2025/301/VO.html.

[4] Council of the European Union. Council Recommendation of 23 May 2024 on enhancing research security. Council Recommendation OJ C/2024/3510, Council of the European Union, May 2024. URL https://eur-lex.europa.eu/eli/C/2024/3510/oj.

[5] DAAD, Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi). KIWi-Checkliste Wissenssicherheit. Checkliste / handreichung, Deutscher Akademischer Austauschdienst (DAAD), 2025. URL https://www.daad.de/de/infos-services-fuer-hochschulen/kompetenzzentrum/kiwi-publikationen/kiwi-kompass-checkliste/.

[6] European Commission. Global Approach to Research and Innovation: Europe's strategy for international cooperation in a changing world. Technical Report COM(2021) 252 final, European Commission, DG Research and Innovation, May 2021. URL https://research-and-innovation.ec.europa.eu/system/files/2021-05/ec_rtd_com2021-252.pdf.

[7] European Parliament and Council of the European Union. Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). Regulation (EU) 2021/821, European Union, May 2021. URL https://eur-lex.europa.eu/eli/reg/2021/821/oj.

[8] Fraunhofer-Gesellschaft. Geschäftsordnung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE. ATHENE governance document, 2022.

[9] Fraunhofer-Gesellschaft. Compliance und Verhaltenskodex; Exportkontrolle; Erklärungen zur Zusammenarbeit mit Dritten. Fraunhofer-Gesellschaft (Zentrale), 2024. URL https://www.fraunhofer.de/de/ueber-fraunhofer/compliance.html.

[10] Fraunhofer-Gesellschaft and Goethe-Universität Frankfurt. Vereinbarung zum Beitritt der Goethe-Universität zu ATHENE unter den Bedingungen der Kooperationsvereinbarung vom 28.11.2018. ATHENE governance document, 2022.

[11] Fraunhofer-Gesellschaft and TU Darmstadt and Hochschule Darmstadt. Kooperationsvereinbarung (CRISP/ATHENE). ATHENE governance document, 2018.

[12] Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung von DFG und Leopoldina. Wissenschaftsfreiheit und Wissenschaftsverantwortung.

Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung. Technical report, Deutsche Forschungsgemeinschaft und Nationale Akademie der Wissenschaften Leopoldina, 2022. URL https://www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/11/2022_Empfehlungen_Wissenschaftsfreiheit_Wissenschaftsverantwortung.pdf.

[13] Government of Canada. National Security Guidelines for Research Partnerships; Policy on Sensitive Technology Research and Affiliations of Concern (STRAC). Technical report, Innovation, Science and Economic Development Canada and the federal granting agencies, 2024. URL https://science.gc.ca/site/science/en/safeguarding-your-research.

[14] Hochschulrektorenkonferenz. Leitfragen zur Hochschulkooperation mit der Volksrepublik China. Beschluss des präsidiums, Hochschulrektorenkonferenz (HRK), Präsidium, September 2020. URL https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-07-Internationales/02-07-01-Internationale-Strategie/HRK_Beschluss_Leitfragen_zur_Hochschulkooperation_mit_der_VR_China_9.9.2020.pdf.

[15] Hochschulrektorenkonferenz. Leitlinien und Standards in der internationalen Hochschulkooperation. Beschluss des präsidiums, Hochschulrektorenkonferenz (HRK), Präsidium, April 2020. URL https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-07-Internationales/02-07-01-Internationale-Strategie/HRK_Beschluss_Leitlinien_und_Standards_in_der_internationalen_Hochschulkooperation.pdf.

[16] International Organization for Standardization. ISO 31000:2018 – Risk Management – Guidelines. Technical report, ISO, Technical Committee ISO/TC 262, 2018. URL https://www.iso.org/standard/65694.html.

[17] Alex Joske. The China Defence Universities Tracker. Policy Brief and public database Report No. 23/2019, Australian Strategic Policy Institute (ASPI), International Cyber Policy Centre, 2019. URL https://unitracker.aspi.org.au/.

[18] Max-Planck-Gesellschaft. Internationale Zusammenarbeit – Standortbestimmung und Orientierungsrahmen. Leitlinien zur Ausgestaltung internationaler Kooperationen der Max-Planck-Gesellschaft. Leitlinien, Max-Planck-Gesellschaft, 2024. URL https://www.mpg.de/16767044/mpg-leitlinien-int-kooperationen-2024.pdf.

[19] Haya Schulmann. ATHENE Cybernation Deutschland – Sicherheit der IT der Universitäten (Lagebild-Bericht 2025). Lagebild-bericht, ATHENE – National Research Center for Applied Cybersecurity, December 2025. URL https://www.athene-center.de/fileadmin/Studien/ATHENE-Lagebild-Bericht-Unis.pdf.

[20] The Royal Society. Science in the Age of AI: How Artificial Intelligence is Changing the Nature and Method of Scientific Research. Technical report, The Royal Society, London, October 2024. URL https://royalsociety.org/science-in-the-age-of-ai.

[21] TU Darmstadt and Fraunhofer-Gesellschaft and Hochschule Darmstadt. Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO. ATHENE governance document, 2020.

[22] University Foreign Interference Taskforce. Guidelines to Counter Foreign Interference in the Australian University Sector. Technical report, Australian Department of Ed-

ucation and the university sector, 2021. URL https://www.education.gov.au/countering-foreign-interference-australian-university-sector.

[23] University-Industry Demonstration Partnership. Export Control Regulations and the University Fundamental Research Exemption. Working document, U.S. National Academies (hosted), 2008. URL https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_055551.pdf.

[24] Fabio Urbina, Filippa Lentzos, Cédric Invernizzi, and Sean Ekins. Dual use of artificial-intelligence-powered drug discovery. *Nature Machine Intelligence*, 4:189–191, 2022. doi: 10.1038/s42256-022-00465-9.

[25] U.S. Department of Commerce, Bureau of Industry and Security. Export Administration Regulations, 15 CFR Part 734 (Scope; §734.8 fundamental research; §734.13–734.15 export and deemed export). 15 CFR Part 734 (eCFR / Cornell LII), 2024. URL https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734.

[26] Wissenschaftsrat. Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche. Positionspapier Drs. 2485-25, Wissenschaftsrat, May 2025. URL https://www.wissenschaftsrat.de/download/2025/2485-25.pdf.

Imprint

Contact

National Research Center for Applied Cybersecurity ATHENE
c/o Fraunhofer Institute for Secure Information Technology SIT
Rheinstraße 75, 64295 Darmstadt, Germany

© Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., München, 2026

Legal entity

ATHENE is a legally non-independent institution of the Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastraße 27c, 80686 München, Germany.
Register of associations: Amtsgericht München (Munich Local Court), VR 4461
Authorized to accept service: Prof. Dr.-Ing. Holger Hanselka (President)

Notes

This document was supported by funding from the Federal Ministry of Research, Technology and Space (BMFTR) and the Hessian Ministry of Science and Research, the Arts and Culture (HMWK) within their joint funding of the National Research Center for Applied Cybersecurity ATHENE.

The results presented in this document have been prepared with care and on the basis of the known state of scientific knowledge. This document describes legal requirements as understood at the date of publication; for specific legal questions, consult the relevant compliance function. No liability or guarantee is assumed that the results or information meet the requirements of the current legal situation. The same applies to their usability, completeness, or freedom from error, so that any liability for damages arising from the use of these results or information is excluded. This limitation of liability does not apply in cases of intent.

This work, including all its parts, is protected by copyright. Any use beyond the narrow limits of copyright law is inadmissible and punishable without the written consent of the Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. The reproduction of trade names and brand names in this document does not imply that such names are to be regarded as free within the meaning of trademark law and may therefore be used by anyone.