NCC-IS Cybersecurity Grant Handbook

Rules and Guidelines for Applicants

Spring 2025

Unofficial Translation

In case of any discrepancies, the Icelandic version of the NCC-IS Cybersecurity Grant Handbook shall prevail

Table of contents

1. Introduction

The NCC-IS Cybersecurity Grant Handbook is intended for applicants and other stakeholders. It is updated for each advertised application deadline and is valid for that specific period. The Handbook aims to clarify the process for all involved, including the application deadline and the management of the awarded grants. It contains grant award rules and useful information on the rights and obligations of beneficiaries. Applicants are encouraged to familiarize themselves with the Handbook. The allocation rules are available in Icelandic on the Eyvor (NCC-IS) website.

The NCC-IS Cybersecurity Grant[1] is under the authority of the Minister of Transport and Local Government[2] and is awarded based on Article 42 of the Public Finance Act, No. 123/2015. The grant is jointly funded in equal measure by the European Union's Digital Europe programme (DIGITAL) and the Ministry. Its purpose is to support projects in the field of cybersecurity in Iceland. The grant aims to strengthen the integration and implementation of new cybersecurity solutions and their design among Icelandic companies and public entities."

The grant is allocated by the National Coordination Centre of Iceland referred to as Eyvor (NCC-IS) and administered by Rannis. Applications for the grant are evaluated based on the current role and focus of Eyvor and their alignment with Specific Objective No. 3 of the Digital Europe Work Programme 2021–2022. This objective aims to ensure extensive implementation and knowledge of cybersecurity solutions across European countries. Special emphasis is placed on building knowledge and implementing the latest online security solutions among SMEs, as well as increasing cooperation between the private and public sectors in accordance with Iceland's Cybersecurity Policy 2022 – 2037.

Eyvor is part of the network of National Coordination Centres (NCCs) within the European Cybersecurity Competence Centre (ECCC). This support function aims to meet the objectives of the ECCC, as defined in Regulation (EU) 2021/887 from the European Union.

The Board of Eyvor is responsible for allocating cybersecurity grants and operates independently in its work.

[1] Hereafter referred to simply as the grant.
[2] Hereafter referred to simply as the ministry.

Application Deadline

- The next deadline is the **March 17, 2025, at 3:00 PM GMT**. The application results are expected six weeks after the deadline.
- Each application deadline is announced and published on the websites of Eyvor, Rannis and on the European Commission's Funding and Tenders portal with at least two months' notice.

2. Rules and Guidelines

The Cybersecurity Grant is a competitive grant awarded based on the Board's focus and the professional assessment of the quality of the projects applied for. The grant supports projects that promote cybersecurity in line with the objectives of Eyvor and ECCC.

If applicable, applicants should state in the application whether the project contains elements that need to be examined regarding the General Code of Ethics and the Icelandic Data Protection Act. In such cases, it is necessary to explain which part of the project potentially violates the General Code of Ethics and/or Data Protection Act, and how the risk will be mitigated. The grant agreement is not finalised until all necessary permission is obtained. Applicants must respect international rules and statutes where appropriate, such as those concerning the exploitation of patents.

2.1 What Parties are Eligible?

The Cybersecurity Grant is intended for Icelandic micro, small and medium-sized enterprises (SMEs) as defined by the EU, as well as public bodies regardless of size, to strengthen their cybersecurity. In this context, the definitions set out in the Commission Recommendation 2003/361/EC of May 6, 2003, of micro, small and medium-sized enterprises (SMEs) apply:

- Medium-sized enterprises: Fewer than 250 employees and turnover below EUR 50 million or a balance sheet below EUR 43 million.
- Small enterprises: Fewer than 50 employees and a turnover or balance sheet below EUR 10 million.
- Micro enterprises: Fewer than 10 employees and a turnover or balance sheet below EUR 2 million.

Companies classified as small or medium-sized enterprises (SMEs) may apply for the grant, even if they are part of a larger group. Cooperation between private companies and public

bodies is encouraged, particularly for those operating within critical infrastructure. However, companies can also apply independently without a partner. Applications that involve collaboration between two legal entities receive a 5% higher score. If the project includes purchased services, the contractor providing those services should not be a co-applicant..

2.2 Type and Sum of Grant

The maximum grant amount is ISK 9,000,000 per project. Beneficiaries are required to contribute at least 20% of the total project cost. The actual total project cost must be at least equal to the grant amount received, plus the beneficiary's contribution. If applicable, all previous funding received for the project from other sources (e.g., state, municipality, European Union, or other public bodies) must be specified in the application. The Cybersecurity Grant does not support costs already covered by other public grants. Therefore, it is not possible to apply for a grant for costs incurred before the application deadline or for costs already financed by other means. The grant falls within the European Commission's *de minimis* aid category. The *de minimis* aid regulation authorises the granting of aid up to EUR 300,000 to each recipient over a period of three years. For government grants covered by *de minimis* aid, beneficiaries declare that they have not received in the last two fiscal years, in addition to the current fiscal year, grants from public authorities which constitute minor aid, an amount exceeding EUR 300,000 including the grant applied for. If the total grant of the *de minimis* aid, including the grant applied for, exceeds EUR 300,000, the beneficiary cannot receive any part of the grant applied for. When assessing whether the limit referenced above is reached, the grant equivalent of aid granted in forms other than direct grants (e.g. loans on favourable terms) shall be calculated according to the rules of the EFTA Surveillance Authority. In this context, however, special grants received by a party according to support rules adopted by the EFTA Surveillance Authority are excluded.

2.3 Eligible Cybersecurity Themes

The Cybersecurity Grant supports projects related to the design, development, and implementation of new cybersecurity solutions. The grant aims to help Icelandic companies enhance their existing cybersecurity capabilities by introducing new solutions. Projects should also aim to increase knowledge and awareness of the importance of cybersecurity in Iceland. The focus of the grant is determined for each allocation and is based on the following six themes:

- Robust cybersecurity culture and awareness
- Effective education, research and development
- Secure digital service and innovation
- Stronger law enforcement, defence and national security

- Effective response to incidents
- Robust infrastructure, technology and legal framework

2.4 Eligible Project Costs

Eligible costs are determined based on the priorities of each allocation and should align with the tasks undertaken to achieve the project's objectives (see the next section for further details). Beneficiaries must maintain their accounts in accordance with Act No. 145/1994 on Accounting, ensuring that the use of funds can be easily traced through project accounting.

3. Costs

3.1 Wages and Wage-related Expenses

The Cybersecurity Grant supports salaries for work on the project. While not all project participants need to be named when submitting an application, the work contribution of all participants for whom wages are requested must be defined in the application. The Cybersecurity Grant does not support the payment of salaries for participants already engaged in full-time employment on other projects. Participants must be dedicated to the cybersecurity project for at least 30% of Full-Time Equivalency. Applicants should consider general collective salary and institutional agreements when calculating salaries; contractor rates cannot be used as a reference. Salary costs should be based on paid salaries and salary-related expenses.

3.2 Other Costs

Other costs include necessary supplies, such as equipment or leasing costs related to the project, as well as travel and contracted services. Contracted services must be described in the 'Project Description' section of the electronic application system, whether provided by an institution or a company. Applicants must explain the nature of the contracted services or advice, the reason for contracting the specific party, and the cost of the service. The Grant may cover the costs of specialized equipment required for the project. It is also permissible to include costs incurred for equipment or product leasing or subscription licenses based on actual costs during the project period. However, this support does not cover general office equipment. The need for the equipment or product must be detailed in the 'Project Description,' along with a rationale for its selection. All costs must be reported in the appropriate fields under ‘2.2 Costs’ of the electronic application system. Unexplained costs will not be approved and any major changes in the cost plan must be approved by the

Cybersecurity Grant administrator. It must be possible to trace costs and therefore it is necessary for costs to be recorded (e.g. in a spreadsheet) for financial reporting and auditing.

Examples of eligible cybersecurity projects:

- **Promoting a culture of cybersecurity and awareness**: Encourage a proactive approach to cybersecurity through continuous education and awareness programs.
- **Effective education, research and development**: Invest in comprehensive education, cutting-edge research, and innovative development in the field of cybersecurity.
- **Secure digital services and innovation**: An innovative company can apply to develop methods or solutions that could be offered as a service.
- **Stronger law enforcement, cyber defence and national security**: Bolster cyber defense capabilities and national security through robust law enforcement measures.
- **Develop Effective Incident Response Strategies**: Implement resilience stress tests, ethical hacking, and response exercises to prepare for cyber threats. Encourage partnerships between companies and organizations to conduct cybersecurity simulations.
- **Stronger infrastructure, technology and legal frameworks**: Enhance the technological infrastructure and legal frameworks to support cybersecurity initiatives.
- **Implement Data Protection Solutions**: Utilize data backups, external hard drives, and cloud solutions to safeguard data.
- **Create or Improve Cybersecurity Plans**: Develop comprehensive cybersecurity plans tailored to organizational needs.
- **Promote Stakeholder Cooperation**: Foster collaboration among stakeholders to address cybersecurity challenges effectively.
- **Prepare for Cybersecurity Certification**: Equip companies and individuals with the knowledge and skills needed to obtain certifications such as ISO/IEC 27001 or CISSP.

Examples of eligible activities:

- **Salary and Personnel Costs**: The grant will support work dedicated to the project. Participants can allocate between 30% and 100% of their Full-Time Equivalency to the project.
- **Cybersecurity Training**: Provide training for employees, including IT and security managers, and system administrators, as part of a comprehensive cybersecurity plan.
- **Contracted Services**: Engage specialist services and cybersecurity counseling to enhance project outcomes.
- **Equipment and Infrastructure**: Purchase or rent equipment and infrastructure necessary for cybersecurity.
- **Travel and Event Participation**: Cover travel expenses and participation in events or training related to the project.
- **Subscription Licenses**: Obtain licenses for cybersecurity software and other similar subscriptions.

3.3 Ineligible Costs

The Cybersecurity Grant cannot be used for overhead costs[3] or for services contracted from parties with a conflict of interest, such as companies or individuals directly linked to the beneficiary. Stakeholders may include, for example, a company board member, CEO, President, Managing Director, General Manager, employee, a close family member etc. The beneficiary is responsible for disclosing all potential conflicts of interest. Examples of ineligible costs:

- Overhead costs.
- Costs not directly related to the project.
- Activities that do not align with the project's objectives.
- Subjects not addressing cybersecurity risks or threats.
- Services contracted from companies or parties with a conflict of interest.
- Costs related to the purchase or upgrade of equipment not relevant to the project.
- Cybersecurity insurance.
- Costs of shipping equipment, machinery, etc.
- Costs of repair and maintenance of equipment and facilities.

[3] Overhead costs, which are fixed and not directly related to the project, arise from the operator's activities. These include expenses for premises such as rent, heating, electricity, management of business units, purchase of books and magazines, and operation of computer equipment."

3.4 Contracts and Procurement Rules

The beneficiary must comply with the General Procurement Act (Government Procurement Act No. 120/2016) and ensure all procurements are conducted efficiently. This includes, for example, soliciting offers from multiple suppliers for products and/or services and comparing prices. All procurement activities and related documentation must be justified, retained, and provided to the Cybersecurity Grant administrator upon request.

4. Preparation of Applications

Applications are accepted via Rannis' electronic application system. The electronic application form is available in both Icelandic and English, and applications can be submitted in either language. However, the project name and a brief description must be provided in both Icelandic and English, as this information will be made public. No documents or amendments will be accepted after the application deadline has passed. If the application is a follow-up for an ongoing project, the progress of the project must be reported in the "Project Description." Each application is assigned a reference number, which can be used in communications with Rannis..

4.1 Project Description

The "Project Description" is accessible in the electronic application system. It must include the product(s) or solution(s) the project aims to deliver, their intended use, the likely end-users, and the extent to which the product(s) or solution(s) will enhance cybersecurity. The current project status and progress towards milestones and deliverables should be clearly stated. It is important to include the following:

- The objectives of the project; impact on cybersecurity and society; innovation: feasibility; status of the project and cooperation with other partners, if applicable.

Applicants are required to write a clear and concise "Project Description" to enable the expert panel to assess the project based on the information provided. If the expert panel cannot understand the project from the description, the application will be dismissed and will not receive evaluation. The "Project Description" must not exceed 10,000 characters.

The project manager, who is responsible for applying for the Cybersecurity Grant and for the execution of the grant contract, both financially and practically, must be specified. Rannis employees will only respond to inquiries about specific projects from the designated project manager. The project manager, managing director/CEO, or the board of the organization may appoint a new project manager during the project. In the case of a collaborative project, all co-applicants must confirm the new project manager, and this announcement must be

submitted to Rannis for confirmation. The final decision to change the project manager is subject to approval by Rannis staff.

4.2 Accompanying Documents

Applicants may submit a link to a video presenting their project. The video should be no longer than **five minutes**. Acceptable platforms include YouTube, Vimeo or similar services. The video must remain accessible until grant decisions are announced.

A presentation slideshow, up to a maximum of **10 slides** (including cover page, references, etc.) should be prepared in PowerPoint or similar program. The presentation must be submitted in PDF format when, with a file size not exceeding 10 MB. Slides should be simple, clear, concise and free of dense text.

The CV of the project manager shall be attached to the electronic application. Documents other than those mentioned above are not allowed.

4.3 Confidentiality

Applications, including attachments and evaluation sheets, are classified as confidential. This data is used exclusively for the assessment of applications and is accessible only to grant administrators, the expert panel, and the Board of Eyvor for evaluation purposes. All application documents and evaluation sheets are retained in Rannis case files. However, a short description of the project and the project name are excluded from confidentiality and will be published in Icelandic and English on the Rannis allocation website and the Eyvor website. Applicants must ensure that the project description and project name do not contain any sensitive information that could potentially cause security or financial harm to the company. All parties involved in the processing and evaluation of applications for Cybersecurity Grants are subject to confidentiality. Applicants may request that certain individuals not read their application by indicating this on the application form. Such requests will be considered by grant administrators and may pertain to members of the expert panel or the Board, as specified in section 1.2 of the application form.

5. Expert Panel Evaluation

The Cybersecurity Grant expert panel assesses applications based on the evaluation criteria, considering the role and aims of the grant. A prerequisite for expert evaluation is that the application is based on a well-developed concept with practical value and likely benefits. Applications that do not meet the minimum formal requirements of the grant will be dismissed before reaching the expert panel.

The Board of Directors of Eyvor is authorized to obtain outside expert opinions when assessing applications, if deemed necessary. In such cases, full confidentiality is maintained. Expert evaluation of applications is based solely on the information provided in the applications and related supporting documents. When assessing applications, the quality of the project is prioritized. Applications must contain a detailed description of:

- The aim of the project, the impact on cybersecurity and society, innovation and feasibility.
- Time and work schedule, milestones, methods and current situation regarding the challenges/risks addressed in the application.
- Project management: Identify the project manager responsible to Eyvor for the implementation of the contract.
- Whether the company or organisation falls within the definition of critical infrastructure according to Act no. 78/2019 on the security of network and information systems of critical infrastructures. Applicants meeting this definition will receive a more favorable assessment (5%).
- The intended publication or presentation of the results.

If the applicant benefits from other grants or contributions for the project, this is to be stated in the application.

5.1 Evaluation Criteria

Evaluation criteria are defined in accordance with the focus of each allocation and are based on the following:

- Impact.
- Novelty.
- Quality and Practicality.
- Project Management and Collaboration.

Grading Scale of applications:

- A1 Excellent application, almost without weaknesses
- A2 Very strong application, minor weaknesses
- A3 Strong application but minor weaknesses
- B Application with one or more limiting weaknesses
- C Incomplete application, many weaknesses
- X Does not fit into the focus of the fund

Eyvor conducted a survey on cybersecurity in both the public and private sectors in Iceland. The results revealed a lack of employee training in cybersecurity and limited opportunities

for lifelong learning in this field. Therefore, applications for grants aimed at training employees in cybersecurity will receive favorable consideration in the assessment process (5%). Examples of staff training:

- **Increasing cybersecurity awareness among general employees**: This could include courses, awareness campaigns, studies on effective methods to enhance cybersecurity awareness, or the development of cybersecurity content for staff.
- **Enhancing technical training for specialised network, IT or cybersecurity staff**: This could involve technical courses or preparation for cybersecurity certifications such as CISSP, Security+, etc.

Other elements that can strengthen an application:

1. **Cybersecurity**: How relevant is the knowledge acquired, or the solutions developed to cybersecurity?
2. **Benefits for industry**: Does the project implement a solution that enhances the industry's or sector's cybersecurity competence? Does the "Project Description" specify the partners involved in the project?
3. **Cross-sectoral knowledge sharing**: Does the solution improve knowledge, experience, and data exchange in cybersecurity across different industries or public sectors?
4. **Novelty**: Does the project involve developing an innovative cybersecurity solution, such as in hardware or software?
5. **Focus on small and medium-sized enterprises**: Does the project benefit small, medium-sized enterprises or public entities in the same category?
6. **Risk assessment**: Have potential risks affecting the project been assessed, and is there a plan to mitigate them?
7. **Feasibility**: To what extent can the project be expected to generate value based on the invested capital, including the likelihood of achieving its objectives efficiently and economically?

5.2 Expert Panel and Board of Directors

The Cybersecurity Grant expert panel consists of six experts with knowledge of cybersecurity who will assess and grade applications. Three experts will evaluate each application individually. If an expert panel member is deemed ineligible to evaluate an application due to a conflict of interest, other expert panel members will be assigned to assess the application. The ineligible expert panel member must also withdraw from any meetings where the application in question is discussed, in accordance with Article 3 of the Administrative Procedures Act No. 37/1993.

Rannis suggests the selection of the expert panel Chairperson, who is then approved by the Board. The Chairperson, with the assistance of the grant administrator, is responsible for coordinating the work of the expert panel and ensuring it functions according to the policy and role of the Cybersecurity Grant and the General Code of Ethics. The names of the expert panel members and the Board of Eyvor are published on the websites of Rannis and Eyvor. The expert panel's evaluation of applications will always be based on the Board's priorities and the quality of the applications. Applicants may under no circumstances contact expert panel members or the Board during the evaluation process. If the applicant contacts an expert panel or Board member concerning an application, the application will be removed from the assessment process without further justification.

6. Grant Award and Contract for Project Implementation

6.1. Award Decision

The expert panel evaluates applications and submits a written report to the Board of Eyvor, prioritising applications based on the expert evaluation. The Chairperson of the expert panel will present the evaluation results to the Board of Eyvor. The Board will then decide on the allocation of grants and make proposals to the Minister of Transport and Local Government, who confirms and signs the grants.

Once an allocation is made, applicants will receive a response letter with the expert panel's final assessment. All applicants will be informed about the processing of their application. Information on grants is published on the Eyvor and Rannis websites. Decisions on awarding grants from the Cybersecurity Grants are final at the administrative level. If applicants have comments on the expert panel's evaluation after allocation, they should direct them to the grant administrator at Rannis.

6.2 Payments for Sponsored Projects

Payments from the Cybersecurity Grant are as follows:

- First payment (80%): Initiated after signing the contract.
- Final payment (20%): Initiated after the final report has been submitted and approved, and a presentation of the project has been delivered (see further details below).

If the combined applications exceed the total financial resources of the grant, grants will be awarded based on the expert panel grading (cf. 5.1). Applications that receive the highest evaluations will be given priority. To ensure fairness, priority is given to applicants who have

not previously received an Eyvor grant. While multiple applications are allowed, only one grant will be awarded per applicant. Rannis may withdraw the contribution and demand reimbursement if the beneficiary fails to comply with their obligations or if there is significant non-performance towards the project and its deliverables.

6.3 Specifying Support and Dissemination of Results

The Cybersecurity Grant is partly financed by the European Union. Beneficiaries are required to present the main results of their project in September 2025. All presentations, publications, and dissemination of the project's results must state that the project is supported by the European Union and the Eyvor Cybersecurity Grant. The Eyvor logo, which is used for the Cybersecurity Grant, can be found on the Rannis and Eyvor (NCC-IS) websites. The European Union logo and detailed guidance on its use can be found in the eu-Emblem-rules_en.pdf (europa.eu) document.

7. Follow-up

The Rannis administrator, on behalf of the Cybersecurity Grant, is responsible for the follow-up of projects and the payment of contributions under the authority of the Board of Eyvor. During the follow-up of accepted contracts, the grant administrator may request a progress report. However, generally, only a final report is requested, indicating the project's outcomes and results.

7.1 Project Manager and Communications

The project manager is responsible for maintaining separate cost accounting for each participant in a project supported by the Cybersecurity Grant. The project manager must always have an overview of the total project cost and provide Rannis with access to accounting documents upon request. Project managers are encouraged to make appropriate changes to the project plan during the work period if it serves the project's interests. However, significant changes to the project plan, budget, or partners during the work period require the approval of the grant administrator. Rannis may withdraw the contribution and demand reimbursement if significant changes are made without its approval.

7.2 Final Report

The final report for the project must be submitted no later than August 20, 2025, although it can be submitted earlier if it fits the project's scope. The final report is completed and submitted electronically through Rannis' electronic application system. The report should

detail the project's progress and any deviations from the original plan. It must be accompanied by an accounting record and detailed statements of expenditure, specifying all costs incurred in connection with the project. Once the final report has been approved, no further costs for the project can be submitted. Before the grant is awarded, a cost evaluation of the project may be conducted, which could affect the grant award.

7.3 More Information

The grant administrator at Rannis is available to provide further information and assistance on weekdays from 9am to 3pm. General questions regarding the grant and applications under evaluation should also be directed to the grant administrator at ncc@rannis.is.