NCC-IS Cybersecurity Grant Handbook

Rules and Guidelines for Applicants

Autumn 2024

Unofficial Translation

In case of any discrepancies, the Icelandic version of the NCC-IS Cybersecurity Grant Handbook is the definitive version

Table of contents

1. Introduction

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

The NCC-IS Cybersecurity Grant[1] (the Grant) is under the authority of the Minister of Higher Education, Industry and Innovation (the Ministry)[2] and is awarded based on Article 42 of the Public Finance Act, No. 123/2015. The grant is jointly and in equal measure funded by the European Union's Digital Europe programme (DIGITAL) and by the Ministry. The role of the Grant is to support projects in the field of cybersecurity in Iceland. The Grant is intended 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, Eyvor NCC-IS and Rannis[3] administers the Grant. Applications for Grants are evaluated based on the role and focus of Eyvor NCC-IS at any given time and whether the application contributes to the specific objective No. 3 of the Digital Europe Work Programme 2021 – 2022, which aims to ensure extensive implementation and knowledge of cybersecurity solutions in European countries. There is special emphasis on knowledge building 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 NCC-IS is part of the network of NCCs, the European Cybersecurity Competence Centre (ECCC), and this support function is intended to meet the objectives of the ECCC, as defined in Regulation (EU) 2021/887 from the European Union.

The Board of Eyvor NCC-IS is responsible for the allocation of the cybersecurity grants and is independent in its work.

[1] Hereafter referred to simply as the Grant.
[2] Hereafter referred to simply as the ministry.
[3] Rannís is short for Rannsóknarmiðstöð Íslands. The English term for the institution is the Icelandic Centre for Research.

Application Deadline

- The next deadline is the **1st of October 2024 at 3pm GMT**. The grant allocation is expected to take place eight weeks after the application deadline.
- Each application deadline is announced and published on the website of Eyvor NCC-IS, 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 and is awarded according to 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 NCC-IS 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 thereof is to be mitigated. The grant agreement is not finalised until all necessary permissions are available. The applicant must respect international rules and statutes where appropriate, for example on 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 in the same size category, 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.

If in doubt about the company or public body size classification, Rannis proposes that applicants undergo the SME self-assessment questionnaire to verify the classification. The definition and procedures for confirming the size of the enterprise can be obtained if there is doubt that the enterprise or public body is classified as small, medium or large.

Cooperation between private companies and public bodies is encouraged, if they operate within critical infrastructures, but companies can also apply without public sector involvement.

2.2 Type and Sum of Grant

The maximum grant sum can be ISK 9,000,000 per project. A 20% contribution towards the project by beneficiaries is also required for each allocation. In other words, the beneficiary must finance at least 20% of the total cost of the project applied for. The actual total project cost must be at least equal to the amount of the grant amount received, in addition to the beneficiary's contribution towards the project. If applicable, all funding that the project has previously received from other sources, e.g. from a state, municipality, the European Union or other public bodies, must be specified in the application. The Cybersecurity Grant does not provide support for costs for which the applicant has already received other public grants for. That is, it is not possible to apply for a grant for costs incurred before the application deadline and it is not possible to apply for a grant for costs that have been financed by other means.

The Cybersecurity 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 cybersecurity-related projects that contribute to the design, development, and implementation of new cybersecurity solutions. The grant should lead to Icelandic companies improving their existing cybersecurity capabilities through the

introduction of new solutions, and the projects should be designed to increase knowledge and awareness of the importance of cybersecurity in Iceland. The focus of the grant is decided 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 based on the priorities of each allocation and should be consistent with the tasks undertaken to achieve the objectives of the project (see next Section for further details). Beneficiaries must keep their accounts in the manner stipulated in Act No. 145/1994 on Accounting and in such a way that the use of the funds can be traced in a straightforward manner from project accounting.

3. Costs

3.1 Wages and Wage-related Expenses

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

3.2 Other Costs

Other costs include the costs of necessary supplies, such as equipment or leasing costs related to the project, as well as travel and contracted services. Contracted services shall be described in the “Project Description” in the electronic application system, whether it is delivered by an institution or a company. Applicants must explain what is involved in the contracted services or advice, why they are contracted from the party in question and the

cost of the service. The Grant may be used to cover the costs of specialised equipment required for the project. It is also permissible to include costs incurred in connection with equipment or product leasing or subscription licenses according to actual costs during the project's period. However, this support does not cover general office equipment. The need for the equipment or product in question must be explained in the "Project Description" and a rationale for its selection provided.

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.
- Effective education, research and development.
- Secure digital services and innovation. Example: 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.
- The development of effective responses to incidents and threats. Example: cybersecurity resilience stress tests, ethical hacking and response exercises for cyber threats. Several companies or organisations partner to conduct a cybersecurity simulation.
- Stronger infrastructure, technology and legal frameworks.
- Data protection-related solutions such as data backups, external hard drives and cloud solutions.
- Develop or improve a cybersecurity plan.
- Promote cooperation between stakeholders in cybersecurity issues.
- Preparation of a company or individual for a cybersecurity certificate (e.g. ISO/IEC 27001, CISSP etc.).

Examples of eligible activities:

- Salary and personnel costs, assuming the Grant will only support work devoted to the project. However, it is permissible that the time commitments of a given participant are between 30% and 100% of Full-Time Equivalency devoted to the project.
- Training in cybersecurity for employees, such as IT and security managers, and system administrators as part of a cybersecurity plan.
- Contracted services, such as specialist services in cybersecurity.

- Purchase or rental of equipment and/or infrastructure related to cybersecurity.
- Travel expenses and participation in events or training related to the project.
- Subscription licenses, e.g. for cybersecurity software.

3.3 Ineligible Costs

The Cybersecurity Grant may not be used for overhead costs and not for costs arising from services contracted from a party where there is conflict of interest, e.g. by companies or individuals directly linked to the beneficiary. Stakeholders can be, for example, a company board member, CEO, President, Managing Director, General Manager, an employee and/or a close family member. The beneficiary is responsible for providing all necessary information on possible conflicts of interest.

Examples of ineligible costs:

- Overhead costs.
- Costs that are not directly related to the project.
- Activities that are not in line with the objectives of the project.
- A subject not addressing cybersecurity risks or threats.
- Services contracted from a company or party where there is conflict of interest.
- Costs related to the purchase or upgrade of equipment that is not related to the project.
- Cybersecurity insurance.
- Costs of shipping of equipment, machinery, and so on.
- Costs of repair and maintenance of equipment and facilities.
- Cybersecurity certification fees (e.g. ISO/IEC 27001, CISSP etc. Although costs related to preparation of a certificate are eligible).

3.4 Contracts and Procurement Rules

The beneficiary shall comply with the General Procurement Act (Government Procurement Act No. 120/2016) and all procurements shall be carried out in the most efficient manner. This includes, for example, requesting offers from more than one supplier regarding products and/or services and making price comparisons. The procurement and documentation relating to tender requests must be justified, retained and delivered to the Cybersecurity Grant supervisor upon request.

4. Preparation of Applications

Applications are accepted via Rannis' electronic application system. An electronic application form can be accessed in both Icelandic and English and applications can be submitted in either language. However, the project name and a brief description are required in both Icelandic and English. No documents or amendments will be accepted after the application deadline has passed. If an application is a follow-up application for a project already started, the progress of the project must be reported in the "Project Description." All applications are assigned a reference number that can be used in communications with Rannis.

4.1 Project Description

The "Project Description" is accessible in the electronic application system. The description must include the product(s)/solution(s) that the project is intended to deliver, how it is to be utilised, who are the likely end-users and to what extent the product(s) or solution(s) are likely to enhance cybersecurity. The current project status and progress towards milestones and deliverables should be clearly stated. It is important that the following be included:

- 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" so that the expert panel can assess the project according to the information provided. If the expert panel is unable to understand the project by reading the description, the application is dismissed and will not receive evaluation. The Project description is not to 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, shall be specified. Rannis employees do not respond to inquiries about specific projects except from a project manager. The project manager, managing director/CEO or board of the organisation may appoint a new person to take over as a project manager during the project. In the case of a collaborative project, all co-applicants shall 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 the approval from Rannis staff.

4.2 Accompanying Documents

Applicants can send a link to a video where the project is presented. The video should not be longer than **five minutes**. Applicants can use video streams such as Youtube, Vimeo or other equivalents. The video file shall be accessible until grant decisions are announced.

A presentation slideshow up to a maximum of **10 slides** (including cover page, references, etc.) to be prepared in PowerPoint or similar program may also be included. The presentation should be in PDF format when it is submitted. The file size must not exceed 10 MB. It is desirable that slides be simple, clear, and concise.

The CV of the project manager shall be attached to the electronic application.

To ensure equal treatment of all applicants, applications where the above rules are not followed are rejected. Other documents are not allowed.

4.3 Confidentiality

Applications, including attachments and evaluation sheets, are classified as confidential. That data is used exclusively for the assessment of applications and is not accessible to anyone other than grant administrators, the expert panel and the Board of Eyvor NCC-IS, for the purpose of assessing the applications. All application documents and evaluation sheets are kept in Rannis case files. A short description of the project, as well as the project name, is, however, excluded from confidentiality and is published in Icelandic and English on the Rannis allocation website and Eyvor NCC-IS website. Since the project description and project name are excluded from confidentiality, applicants shall ensure that there is no representation of 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. A request can be made on the application form if there is a wish for a certain individual(s) to not read the application, which will be considered by grant administrators. These can be either a member of the expert panel or the Board, see section 1.2 on the application form.

5. Expert Panel Evaluation

The Cybersecurity Grant expert panel assesses applications based on the evaluation criteria and taking into consideration the role and aims of the Grant. A prerequisite for assessing an application for expert evaluation is that it is based on a well-developed concept of practical value and likely benefits. An application that does not meet the minimum formal requirements of the grant will be dismissed before the expert panel assesses it. The Board of Directors of Eyvor NCC-IS is authorised to obtain outside expert opinion 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 applications and related supporting documents. When assessing applications, the quality of the project is prioritised. Applications shall 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 in terms of the challenges/risks addressed in the application.
- Project management: Identify the project manager responsible to Eyvor NCC-IS for the implementation of the contract.
- Whether the company or organisation falls within the definition of critical infrastructure in accordance with Act no. 78/2019 on the security of network and information systems of critical infrastructures.
- 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 NCC-IS‘s survey on cybersecurity was conducted in both the public and private sectors in Iceland. The results revealed that there was a lack of training of employees in cybersecurity as well as opportunities for lifelong learning in this field. Applications for grants in this area, i.e. those who seek to train their employees in cybersecurity, will therefore receive favorable consideration in the assessment process. Below are some examples of staff training:

- **Increase in cybersecurity awareness of general employees**. For example, courses, an awareness campaign, a study of what could be a good way to increase cybersecurity awareness or the development of cybersecurity content for staff.
- **Increase in technical training of specialised network, IT or cybersecurity staff**. Technical training could include, for example, a course or preparation for cybersecurity certification (e.g. CISSP, Security+, etc.).

Other elements that can strengthen an application:

1. **Cybersecurity**: How likely is it that the knowledge acquired, or solutions developed are of relevance to cybersecurity?
2. **Benefits for the industry**: Does the project involve the implementation of a solution that makes the industry/sector more competent in terms of cybersecurity? Does the "Project Description" include which partners are included in the project?
3. **Cross-sectoral knowledge sharing**: Does the solution improve knowledge, experience and data exchange in cybersecurity between different industries and/or public sectors?
4. **Novelty**: Does the project involve the development of an innovative cybersecurity solution, e.g. in hardware or software?
5. **Focus on small and medium-sized enterprises**: Does the project benefit small and/or medium-sized enterprises or public entities in the same size category?
6. **Risk assessment**: Have risks that could affect 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 invested capital, including whether the project is likely to achieve its objectives in the most efficient and economical way possible?

5.2 Expert Panel and Board of Directors

The Cybersecurity Grant expert panel is composed of five experts with knowledge of cybersecurity that will assess and grade applications. Three experts will evaluate each application individually. If a particular expert panel member is considered ineligible to evaluate an application due to conflict of interest, other expert panel members will be assigned to assess said application. The expert panel member in question must also withdraw from any meetings when the application in question is to be 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 is responsible, with the help of the administrator of the Grant, to coordinate the work of the expert panel and make sure 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 Board of Eyvor NCC-IS are published on the website of Rannis and Eyvor NCC-IS. The evaluation of applications by the expert panel shall always be based on the Board's priorities and the quality of applications.

Applicants may under no circumstances contact expert panel members or 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 NCC-IS where applications have been prioritised based on the expert evaluation. The Chairperson of the expert panel will present the results of the evaluation to the Board of Eyvor NCC-IS. The Board shall decide on the allocation of grants and then make proposals to the Minister of Higher Education, Industry and Innovation, who confirms and signs the grants. When an allocation is made, applicants will receive a response letter with the final assessment of the expert panel. All applicants shall be informed of the processing of the application. Information on grants is published on Eyvor NCC-IS and Rannis websites. Decisions on awarding grants from the Cybersecurity Grants are final at the administrative level.

If applicants have comments on the evaluation of the expert panel after allocation, they shall be directed to the administrator of the Cybersecurity Grant at Rannís.

6.2 Payments of Sponsored Projects

Payments from the Cybersecurity Grant are as follows:

- The first payment process (80%) is initiated after signing the contract.
- The final payment process (20%) is 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 in accordance with expert panel grading, cf. 5.1. Applications that receive the highest evaluation will be given priority. Rannis may withdraw the contribution and demand

reimbursement if the beneficiary fails to comply with their obligations and/or if there is significant non-performance towards the project.

6.3 Specifying Support and Dissemination of Results

The Cybersecurity Grant is partly financed by the European Union and the beneficiaries should have a presentation in September 2025 where the main results of the project are presented. It must be stated in all presentations, publications and dissemination of the results of the project, that the project is partly supported by the European Union and by the Eyvor NCC-IS Cybersecurity Grant. The Eyvor NCC-IS logo is used for the Cybersecurity Grant and can be found on the Rannis and Eyvor NCC-IS websites. The European Union logo and more detailed guidance on its use can be found on the eu-Emblem-rules_en.pdf (europa.eu).

7. Follow-up

The Rannís administrator, on behalf of the Cybersecurity Grant, is responsible for the follow-up of projects and payments of contributions under the authority of the Board of Eyvor NCC-IS. During the follow-up of accepted contracts, the Cybersecurity Grant administrator may request a progress report, but generally only a final report is requested, indicating the outcome and results of the project.

7.1 Project Manager and Communications

The project manager is responsible for maintaining a separate cost accounting for each participant in a project supported by the Cybersecurity Grant. The project manager shall at any time have an overview of the total cost of the project and shall 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 this serves the interests of the project. Significant changes to the project plan, budget or partners during the work period require the approval of Cybersecurity Grant administrator. Rannis can withdraw the contribution and demand reimbursement if significant changes are made without the approval of Rannis.

7.2 Final Report

The final report for the project shall be submitted no later than August 20, 2025, although it is permissible to submit earlier if fits the scope of the project. The final report is completed and submitted electronically in Rannis' electronic application system. The report shall set out the progress of the project as well as any deviations from the original plan. The report

shall be accompanied by an accounting record and detailed statements of expenditure. All costs incurred in connection with the project shall be specified in the final report. Once the final report has been approved, further costs for the project cannot be submitted. Before the Grant is awarded, a cost evaluation of the project may be carried out, which may affect the award of the grant.

7.3 More Information

The administrator of the Cybersecurity Grant at Rannis provides further information and assistance on weekdays from 9am to 3pm. General questions regarding the grant and applications under the evaluation process shall also be addressed to the Cybersecurity Grant administrator at ncc@rannis.is.