



Co-funded by
the European Union

Eyvör Cybersecurity Grant Handbook

Rules and Guidelines for Applicants

Autumn 2026

Unofficial Translation

In case of any discrepancies, the Icelandic version of the Eyvör (NCC-IS) Cybersecurity Grant Handbook (Handbók Netöryggisstyrks Eyvarar) shall prevail.

Table of Contents

1. The Eyvör Cybersecurity Grant	1
1.1 Purpose and legal basis	1
1.2 Governance and administration	1
1.3 Application deadline	2
2. Grant conditions	2
2.1 Who may apply	2
2.2 Lead applicant and co-applicants.....	3
2.3 Grant amount and co-financing.....	3
2.4 Priority areas and eligible projects	4
2.5 State aid and other public funding	4
2.6 Ownership and control.....	5
3. Eligible costs.....	8
3.1 General conditions	8
3.2 Salaries	8
3.3 Purchased services and other costs	8
3.4 Ineligible costs.....	10
3.5 Procurement	10
4. Preparation and submission of applications.....	11
4.1 Application system and formal requirements	11
4.2 Project description.....	11
4.3 Supporting documents.....	11
5. Evaluation process.....	12
5.1 Confidentiality	12
5.2 Conflicts of interest	13
5.3 Expert panel and Board	13
5.4 Expert evaluation and evaluation criteria	14
5.5 Bonus points	15
5.6 Award decision	16
5.7 Notification of results.....	16
6. Grant agreement and payments.....	17
6.1 Grant agreement preparation	17

6.2 Payments	17
6.3 Changes to the project	17
6.4 Publication and dissemination of results	17
6.5 Ownership of results	18
7. Monitoring and final reporting	18
7.1 Project manager	18
7.2 Progress report	19
7.3 Final report	19
7.4 Non-compliance, cancellation and recovery	19
7.5 Further information	19

1. The Eyvör Cybersecurity Grant

This handbook applies to applications for the Eyvör Cybersecurity Grant in autumn 2026. It sets out the conditions of the grant, the preparation and evaluation of applications, the award decision and the obligations of grantees. Applicants are advised to read the handbook in full before applying. The award rules are available in Icelandic on the [Eyvör](#) (NCC-IS) website.

1.1 Purpose and legal basis

The purpose of the Eyvör Cybersecurity Grant is to support projects that strengthen cybersecurity in Iceland. The grant is intended to support the design, development, adaptation and deployment of cybersecurity solutions and to contribute to greater knowledge and skills in the field of cybersecurity. The grant is intended for micro, small and medium-sized enterprises, public bodies and non-profit organisations in Iceland working on projects that fall within the grant's priorities for the call in question.

The Eyvör Cybersecurity Grant is awarded based on Article 42 of the Public Finance Act No. 123/2015. The grant is funded partly by the Icelandic Treasury and partly by the European Union's [Digital Europe Programme](#). Rannís (the Icelandic Centre for Research) administers the grant on behalf of Eyvör.

1.2 Governance and administration

The Cybersecurity Grant is awarded by Eyvör, the National Coordination Centre for Iceland, and administered by Rannís. Applications are assessed considering Eyvör's role and priorities at any given time, and consideration is also given to whether projects support Specific Objective 3 (Cybersecurity and Trust) of Regulation (EU) 2021/694 establishing the Digital Europe Programme. Those objective places particular emphasis on ensuring the wide deployment of, and knowledge of, state-of-the-art cybersecurity solutions across the European economy. The evaluation of applications also considers the priorities set out in the current Digital Europe Cybersecurity Work Programme for 2025–2027.

Emphasis is placed on capacity building and the deployment of cybersecurity solutions in small and medium-sized enterprises. Consideration is also given to projects that promote cooperation between industry and the public sector, in line with [Iceland's National Cybersecurity Strategy 2022–2037](#).

Eyvör is part of the Network of National Coordination Centres of the [European Cybersecurity Competence Centre \(ECCC\)](#), and this support action is intended to fulfil the objectives of

the ECCC as laid down in Regulation (EU) 2021/887 of the European Parliament and of the Council.

The Eyvör Board is responsible for preparing and carrying out Cybersecurity Grant awards and is independent and impartial in its work. The award of grants is subject to ministerial confirmation, see Section 5.6.

1.3 Application deadline

- a. The application deadline is 1 December 2026 at 15:00. The aim is for the award results to be available within six weeks of the close of the call.
- b. The application deadline is announced and published on the websites of Eyvör and Rannís and on the European Commission's EU Funding & Tenders Portal at least two months in advance.

2. Grant conditions

The Cybersecurity Grant is a competitive grant awarded in line with the priorities of the Eyvör Board and based on an expert evaluation of project quality. Applicants must state in their application whether the project involves elements that require consideration with regard to general ethical principles and/or the Act on Data Protection and the Processing of Personal Data No. 90/2018. If the project raises ethical issues, involves the processing of personal data or includes other elements subject to permits or approvals, these must be described in the application, together with an explanation of how the project will be carried out in compliance with applicable laws and regulations. A grant agreement will not be concluded until the necessary permits and approvals have been obtained. Applicants must respect international rules and conventions where applicable, for example regarding the use of patents.

2.1 Who may apply

The Cybersecurity Grant is intended for micro, small and medium-sized enterprises, public bodies and non-profit organisations in Iceland, to strengthen their cybersecurity posture.

An enterprise is considered a micro, small or medium-sized enterprise according to the definition set out in Commission Recommendation 2003/361/EC. When determining the size category of an enterprise, account shall be taken of staff headcount, annual turnover and/or annual balance sheet total, as applicable.

Enterprise category	Staff headcount (AWU)	Turnover or balance sheet total
Medium-sized enterprise	Fewer than 250	Turnover not exceeding EUR 50 million or balance sheet total not exceeding EUR 43 million
Small enterprise	Fewer than 50	Turnover not exceeding EUR 10 million or balance sheet total not exceeding EUR 10 million
Micro enterprise	Fewer than 10	Turnover not exceeding EUR 2 million or balance sheet total not exceeding EUR 2 million

When determining the size category of an enterprise, account shall also be taken of linked enterprises and partner enterprises in accordance with the above EU definition. An enterprise is therefore only eligible under this section if, taking those relationships into account, it qualifies as a micro, small or medium-sized enterprise.

Applicants must also meet the ownership and control conditions, see Section 2.6.

2.2 Lead applicant and co-applicants

An application may be submitted by a single entity or by several entities jointly. If more than one entity is involved in an application, one of them shall be the lead applicant.

The lead applicant is responsible for implementing the project, for communication with Rannís and for submitting documents and reports. The lead applicant must meet the conditions of Section 2.1.

Co-applicants may be enterprises, universities, research institutions, public bodies, non-profit organisations or other legal entities, as appropriate. The application must clearly describe the role of each co-applicant and its contribution to the project.

Only co-applicants established in Iceland that fall within the categories of applicants specified in Section 2.1 may receive a share of the grant. Other legal entities established in an EU/EEA country, such as large enterprises, universities and legal entities in other EU/EEA countries, may take part in the project as co-applicants without receiving a share of the grant, if they fully fund their own participation and project costs. All co-applicants, whether they receive a share of the grant, must meet the ownership and control conditions, see Section 2.6.

2.3 Grant amount and co-financing

The grant may amount to a maximum of ISK 15,000,000 per project and a maximum of 80% of the total project cost. The applicant must therefore provide co-financing of at least 20% of the total project cost. All costs on which the total project cost is based must be recorded

in the accounts. The same cost item cannot form the basis of more than one public grant. It is therefore not possible to apply for a grant for cost items that have already been funded by other public grants or funding.

2.4 Priority areas and eligible projects

The Cybersecurity Grant supports projects in the field of cybersecurity solutions that contribute to the design, development and deployment of new cybersecurity solutions. Projects shall aim to improve the applicant's cybersecurity through the deployment of new solutions and shall be likely to increase knowledge and awareness of the importance of cybersecurity solutions in Iceland. The priorities of the grant are set for each call and are shaped by the following categories:

- Strengthening cybersecurity culture and awareness
- Applied education, research and development
- Secure digital services and innovation
- Robust law enforcement, cyber defence and national security
- Effective incident response
- Strong infrastructure, technology and legal framework

2.5 State aid and other public funding

A grant to an entity that constitutes an undertaking within the meaning of the EEA State aid rules is awarded under the de minimis aid rules¹, in accordance with Commission Regulation (EU) 2023/2831 on the application of Articles 107 and 108 of the Treaty on the Functioning of the European Union to de minimis aid. Applicants that do not constitute undertakings within the meaning of the EEA State aid rules are not subject to the de minimis rules.

The total amount of de minimis aid granted to a single undertaking shall not exceed EUR 300,000 over any period of three years. In assessing whether the ceiling has been reached, all de minimis aid granted to the undertaking during the previous three years shall be considered. When calculating the ceiling, account shall also be taken of other enterprises which, together with the applicant, constitute a *single undertaking* within the meaning of the Regulation.

¹ https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_6567/IP_23_6567_EN.pdf

The applicant is responsible for disclosing all de minimis aid that must be considered when calculating the ceiling. If the proposed grant would result in the ceiling being exceeded, the grant may not be awarded, either in whole or in part. The amount of de minimis aid shall be assessed based on its gross grant equivalent. This applies, among other things, where public aid is granted in a form other than a direct grant, such as a loan on favourable terms. The same costs cannot be funded more than once by public support. The applicant must therefore disclose any other public funding of the project and ensure that support is not sought for costs that have already been funded by other public grants or support.

2.6 Ownership and control

Cybersecurity projects within the Digital Europe Programme may be subject to ownership and control conditions under Article 12(5) and (6) of Regulation (EU) 2021/694, to protect the security interests of the Union and its Member States. The Eyvör Cybersecurity Grants fall within the scope of the Regulation. In accordance with ECCC guidance, Eyvör is responsible for verifying the ownership and control of applicants and grantees.

Who the conditions apply to: The conditions apply to the lead applicant and all co-applicants, including those who fund their own participation without a share of the grant, see Section 2.2. None of them may be controlled, directly or indirectly, by a non-EU/EEA country or by legal entities or natural persons from such a country. EU/EEA means the Member States of the European Union together with Iceland, Norway and Liechtenstein. Entities subject to such control may neither receive a grant nor take part in a project as co-applicants. Guarantees cannot be provided to derogate from this condition.

What control means: Control means the possibility to exercise decisive influence over a legal entity, directly or indirectly through one or more intermediate legal entities, de jure or de facto. It is irrelevant whether that influence is exercised; the possibility alone is sufficient. The assessment considers all levels of the ownership chain, up to the ultimate owners, and includes, among other things, the following factors:

- ownership and special rights attached to shares, such as veto rights or shares with enhanced voting rights;
- governance, in particular who can appoint or dismiss management and approve the budget;
- commercial and financial ties that may give a non-EU/EEA party decisive influence;
- other factors that may confer such control.

For example, a legal entity is considered to be controlled from outside the EU/EEA if its parent company, or a company higher up in the ownership chain, is subject to such control,

even if its direct owners are established in Iceland. The same applies if a non-EU/EEA owner can block strategic decisions, for example because of qualified majority requirements. For natural persons, nationality alone is decisive. A person holding the nationality of both an EU/EEA country and a non-EU/EEA country is considered a national of an EU/EEA country.

Public bodies: Public bodies are controlled by their own state and are not required to submit an ownership and control declaration. In this context, public bodies include:

- the state and its agencies;
- municipalities and their agencies;
- public limited companies (ohf.) and other legal entities wholly owned or controlled by the state or municipalities.

Rannís verifies the status of public bodies based on their Icelandic ID number (kennitala). Private schools and universities, and other legal entities that are not wholly publicly owned, are not considered public bodies in this context and must submit a declaration.

Ownership and control declaration: Small and medium-sized enterprises, non-profit organisations and all co-applicants that are not public bodies must submit with their application a signed ownership and control declaration using the Eyvör form. The declaration must be signed by a person authorised to legally bind the entity, such as a holder of procuration (prókúruhafi) or the board. Electronic signatures are accepted. In the application system, applicants must also:

- list all owners who hold, directly or indirectly, 5% or more of the share capital or voting rights, together with their nationality or country of establishment. Non-profit organisations instead describe how voting rights are structured and whether non-EU/EEA parties hold a majority of votes or a veto;
- state whether the legal entity is controlled, directly or indirectly, by a non-EU/EEA party;
- confirm their commitment to notify Rannís of any changes in ownership or control during the grant period.

An application cannot be submitted if the declaration is missing. A legal entity that declares that it is controlled from outside the EU/EEA is not eligible.

In the declaration, the legal entity confirms, among other things, that it is established in Iceland or, in the case of a co-applicant, in another EU/EEA country. Co-applicants established outside Iceland may, however, only take part under the conditions set out in Section 2.2, i.e. without a share of the grant.

Deadline: The conditions must be met before the application deadline. Changes in ownership or control occurring after that date will not be considered.

Assessment by Rannís: Rannís reviews the declarations during the formal eligibility check of applications, before they proceed to expert evaluation. Information is compared, among other things, with the Register of Enterprises and the register of beneficial owners kept by Iceland Revenue and Customs (Skatturinn). Where ownership is foreign or complex, Rannís may request further documents, such as the shareholder register, articles of association, shareholder agreements and identification documents of the ultimate owners. The provision of documents cannot be refused on grounds of commercial confidentiality. An application will be rejected if:

- the declaration is missing, unsigned, or signed by a person not authorised to legally bind the entity;
- the requested documents are not received within the specified deadline;
- the assessment reveals that the lead applicant or a co-applicant is controlled from outside the EU/EEA, or that ownership is so unclear that such control cannot be ruled out.

Before an application is rejected on these grounds, the applicant will be given the opportunity to comment.

Changes during the grant period: The conditions apply throughout the grant period. The grantee must notify Rannís without delay of any change in ownership or control, for example because of a sale or merger, and submit a new declaration. If the grantee no longer meets the conditions, further payments will be suspended and costs incurred after the conditions ceased to be met are ineligible. Rannís may demand repayment of grant funds paid in respect of such costs, see Section 7.4.

Incorrect information: If it emerges that incorrect or misleading information has been provided about ownership or control, Rannís may reject the application, terminate the grant agreement and demand repayment of the grant.

Processing of personal data: Information about owners, including personal data, is used solely to assess whether the ownership and control conditions are met. It is retained for as long as necessary for the purposes of European Union monitoring and audit, and in accordance with the Public Archives Act. Further information on the processing of personal data can be found in the [Rannís privacy policy](#).

3. Eligible costs

3.1 General conditions

Eligible costs must be consistent with the project's objectives and with the work packages carried out during the project period. Costs are only eligible if they are incurred on or after the date of the application deadline and within the project period. Costs incurred before that date are ineligible.

The project period ends no later than 20 August 2027, cf. the deadline for the final report in Section 7.3. Costs incurred after the end of the project period are ineligible.

Costs incurred before the grant agreement has been signed are at the applicant's own risk.

Applicants are responsible for familiarising themselves with the tax treatment of public grants and are advised to direct any tax questions to Iceland Revenue and Customs (Skatturinn).

3.2 Salaries

The Cybersecurity Grant supports salary costs for work on the project. Not all participants need to be named when the application is submitted, but the work input of all participants for whom salary costs are claimed must be specified in the application. An employee's salary costs are only eligible if their work on the project amounts to at least 30% of a full-time position during the period in which the costs are incurred. When calculating salaries, applicants shall refer to the applicable collective and institutional wage agreements; i.e. billable (external) rates cannot be used as the basis for calculating salaries. Salary costs are based on salaries paid plus employer-related charges.

3.3 Purchased services and other costs

Other costs include the cost of necessary inputs, such as equipment or goods rental for the project, as well as travel costs and purchased services. Purchased services must be described in the application, whether they are provided by an institution or a company. The application must explain what the purchased service or consultancy involves, why it is being purchased from the provider in question and what it costs. If the project involves purchased services, the contractor may not also be a co-applicant. The grant may be used to cover the cost of specialised equipment and devices that need to be acquired for the project. Costs of equipment or goods rental, or subscription licences, may also be claimed at actual cost during the project implementation period. This support does not, however, extend to general

office equipment. The need for such equipment and devices must be explained in the “Project description”, together with the reasons for the option chosen.

All costs must be itemised in the relevant fields under “2.2 Costs” in the electronic application system. Costs must be recorded in a clear and traceable manner, including through timesheets, travel expense reports and other appropriate supporting documents.

Examples of eligible cybersecurity projects (non-exhaustive list):

- Strengthening cybersecurity culture and awareness.
- Applied education, research and development in the field of cybersecurity.
- Secure digital services and innovation. *Example:* start-ups may apply to develop methods or solutions that can be offered as a service.
- Strengthening law enforcement, cyber defence and national security.
- Developing effective responses to incidents and threats. *Example:* Stress testing, *ethical hacking* and cyber threat response exercises. Two or more enterprises or institutions may also join forces to carry out a cybersecurity exercise.
- Strengthening infrastructure, technology and the legal framework.
- Solutions related to data protection, such as data backup and the use of external hard drives and cloud solutions.
- Developing or improving a cybersecurity plan.
- Projects that promote greater cooperation between stakeholders on cybersecurity.
- Preparation for cybersecurity certification or professional certification in the field of cybersecurity, e.g. ISO/IEC 27001 or CISSP.

Examples of eligible activities:

- Salary and staff costs, provided that the grant is used solely for work carried out on the project. An employee's share of a full-time position on a project funded by the Cybersecurity Grant may range from 30% to 100%.
- Cybersecurity training for staff, e.g. for IT and security managers.
- Purchased services, such as expert services and consultancy in the field of cybersecurity.
- Purchase or rental of equipment and/or infrastructure related to cybersecurity.

- Travel costs and participation in events or courses related to the subject of the project.
- Subscriptions and licence fees, e.g. for cybersecurity software.

3.4 Ineligible costs

As a rule, the Cybersecurity Grant may not be used to cover overhead or facility costs², nor to pay for services purchased from parties related to the grantee, such as companies or individuals with a direct financial or personal connection to the grantee. Related parties may include, among others, a board member or alternate, a person with managerial responsibility for the company, an employee and/or a close family member. The grantee is responsible for disclosing any potential conflicts of interest and providing all necessary information on them.

Examples of ineligible costs:

- Overhead and facility costs.
- Costs not directly related to the project.
- Costs of activities that are not consistent with the project's objectives.
- Costs of activities that do not address cybersecurity risks or cybersecurity threats.
- Services purchased from related parties where a conflict of interest exists.
- Costs of purchasing or upgrading equipment not related to the project.
- Costs of cyber insurance.
- Shipping and transport costs for equipment, machinery, etc.
- Costs of repair and maintenance of equipment, devices and real estate.

3.5 Procurement

A grantee subject to the [Public Procurement Act No. 120/2016](#) must comply with its provisions. Other grantees must ensure cost-effectiveness, transparency and traceability in their procurement and be able, upon request, to demonstrate how the choice of supplier and price was determined.

² Overheads are fixed costs that are not directly related to individual projects but arise from the operator's activities. They include premises costs such as rent, heating and electricity, management of operating units, purchase of books and journals, operation of IT equipment etc.

4. Preparation and submission of applications

4.1 Application system and formal requirements

The application and all supporting documents must be submitted through the [Rannís electronic application system](#) before the application deadline. Documents received after the deadline or outside the application system will not be considered unless specifically requested during the processing of the application. Applications may be submitted in Icelandic or English. Applicants may submit more than one application, but only one application from the same applicant can be funded in each call.

4.2 Project description

The “Project description” is part of the electronic application form. It must give a clear account of the outputs the project is expected to deliver, how they will be used, who the likely end users of those outputs are and to what extent the idea is likely to strengthen cyber defences. It must also give a clear account of the status of the project and the path towards its objectives. It is important that the following points are covered:

- The project's objectives,
- impact on cybersecurity and society,
- novelty,
- feasibility,
- status of the project,
- cooperation, where applicable.

The application must be sufficiently clear and detailed to enable the expert panel to evaluate the project based on the information provided in the application and the permitted supporting documents. The maximum length of the “Project description” is 10,000 characters including spaces.

A project manager must be named who is responsible to the Cybersecurity Grant for the implementation of the agreement, both financially and operationally.

4.3 Supporting documents

Applicants may submit a link to a video presenting the project. The video must not exceed **five minutes**. Applicants may use services such as YouTube, Vimeo or other comparable platforms. The video must remain accessible until the award decision has been made.

Applicants may also attach a slide presentation of **no more than 10 slides**, including the title slide, references, etc. The presentation should be prepared in PowerPoint or a comparable program but submitted in PDF format. Files larger than 10 MB will not be accepted. The slides should preferably be simple, clear and concise and should not contain large amounts of continuous text.

The CV of the contact person or project manager must be attached to the application. In addition, small and medium-sized enterprises, non-profit organisations and co-applicants that are not public bodies must attach to the application a signed ownership and control declaration using the Eyvör form, see Section 2.6. No supporting documents other than those specified in this section are permitted.

5. Evaluation process

The expert panel's evaluation of applications shall always be based on the Board's priorities and the quality of the applications. The Cybersecurity Grant expert panel evaluates applications considering the objectives of the grant and the priorities announced for each call. For an application to be eligible for expert evaluation, it must be based on a well-developed idea of the project's practical value and likely benefits. An application will be rejected before it is evaluated on its merits by the expert panel if any of the following applies:

- The application is received after the application deadline
- The application is incomplete, i.e. mandatory fields or sections have not been completed
- The applicant does not meet the eligibility conditions
- The ownership and control declaration is missing, or the lead applicant or a co-applicant does not meet the ownership and control conditions, see Section 2.6
- The grant amount requested exceeds the de minimis ceiling, where applicable, see Section 2.5

The Eyvör Board may, where necessary, seek the opinion of external experts when evaluating applications. In such cases, strict confidentiality shall be maintained. The expert evaluation of applications is based solely on the information contained in the applications and their supporting documents. The quality of the project shall be the overriding consideration in the evaluation of applications.

5.1 Confidentiality

Application documents are treated as confidential during the administration and evaluation of applications. Access to documents is otherwise governed by applicable law, including the

Information Act No. 140/2012. The documents are used solely for the evaluation of applications and are not accessible to anyone other than Rannís staff, the expert panel and the Cybersecurity Grant Board, to the extent necessary for the evaluation of the applications. All application documents and evaluation sheets are kept in the Rannís records management system. However, the project title and summary are exempt from confidentiality and are published in Icelandic and English on the Rannís award page and on the Eyvör website. As this information is published publicly, applicants must ensure that it does not contain information that could cause the company security-related or financial harm. Everyone involved in processing and evaluating Cybersecurity Grant applications is bound by a duty of confidentiality. Applicants may also state in the application form if they specifically request that certain individuals not take part in the review of their application. Rannís staff will not respond to enquiries about specific projects unless they come from the project manager.

5.2 Conflicts of interest

Conflicts of interest (disqualification) of expert panel and Board members are governed by Chapter II of the Administrative Procedures Act No. 37/1993. A member with a conflict of interest shall not have access to the application concerned or take part in its evaluation, discussion or decision. Conflicts of interest and the resulting absence shall be recorded in the meeting minutes. Applicants may also point out a possible conflict of interest of an expert panel or Board member, see item 1.2 of the application form. In such cases, the expert panel or Board member concerned will not have access to the application.

5.3 Expert panel and Board

Rannís nominates six experts with knowledge of cybersecurity to serve on the expert panel. The Eyvör Board appoints the expert panel based on these nominations. The Board also appoints the chair of the expert panel from among its members. The chair, in consultation with Rannís staff, oversees the coordination of the expert evaluation. Each application is evaluated by three expert panel members, one of whom acts as rapporteur and is responsible for the expert panel's consensus summary, which the applicant receives with the response letter. All three panel members score the application, discuss it at an expert panel meeting and reach a joint conclusion on the final score. At the end of the evaluation process, a ranking meeting is held at which the expert panel reviews the applications and ranks them according to the results of the evaluation. Based on this ranking, a ranking list is drawn up of the applications the expert panel recommends for funding, and the list is submitted to the Board for decision. The names of the expert panel members and the Eyvör Board are available on the Rannís and Eyvör websites.

During the evaluation process, all communication from applicants regarding applications shall go through Rannís. Applicants shall not contact expert panel or Board members with a view to influencing the handling or evaluation of an application.

5.4 Expert evaluation and evaluation criteria

The evaluation criteria are defined in line with the priorities of each call; see the [evaluation sheet](#) for the different weightings of the criteria. The basic evaluation can give a maximum of 85 points and bonus points up to 15, so that an application can receive a maximum of 100 points. The evaluation is based on the following criteria:

- Impact
- Novelty
- Quality and cost-effectiveness
- Project management

In assessing the above evaluation criteria, the following points, among others, are considered:

1. **Importance for cybersecurity:** How likely is it that the knowledge acquired or the solutions developed will be of real value for cybersecurity?
2. **Benefit for industry or a sector:** Does the project involve deploying a solution that increases the cyber resilience of industry or of a particular sector? Does the “Project description” state which partners are taking part in the project?
3. **Knowledge sharing between sectors:** Does the project contribute to greater sharing of knowledge, experience and data on cybersecurity between different sectors and/or the public sector?
4. **Novelty:** Does the project involve developing 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?
6. **Risk assessment:** Have the risks that may affect the project been assessed, and are mitigation measures planned to address them?
7. **Cost-effectiveness:** To what extent can the project be expected to deliver value, including whether its objectives are likely to be achieved cost-effectively? In this

assessment, it is relevant, among other things, that salary and consultancy costs are not excessive.

Rating categories / definitions:

- **A1** Meets the evaluation criteria very strongly, with only negligible weaknesses.
- **A2** Meets the evaluation criteria well but has minor weaknesses.
- **A3** Largely meets the evaluation criteria but has some weaknesses that reduce the strength of the application.
- **B** Partially meets the evaluation criteria but has significant weaknesses that limit the quality of the application.
- **C** Does not adequately meet the evaluation criteria and has significant or extensive weaknesses.
- **X** Does not meet the basic conditions of the grant and is therefore not evaluated further.

Applications must include a clear description of:

- The project's objectives, its impact on cybersecurity and society, its novelty and feasibility.
- The timeline and work plan, milestones, methods and status of the project, considering the challenges or risks discussed in the application.
- Project management; a project manager must be named who is responsible to Eyvör for the implementation of the agreement.
- Whether the company or institution falls within the definition of critical infrastructure under the Act on the Security of Network and Information Systems of Critical Infrastructure No. 78/2019, or any legislation replacing it.
- Planned publication or presentation of results.

5.5 Bonus points

Bonus points are added to the application's score; the following items can raise an application's score:

Applications where the project strengthens staff capacity to identify, assess and respond to risks related to the use of artificial intelligence³ receive additional weight in the evaluation (5 points).

Cooperation between companies and public bodies is also particularly encouraged, especially where they operate within critical infrastructure.⁴ An application with at least two independent legal entities as applicants receives 5 bonus points.

A project receives 5 bonus points if the applicant is an operator of essential services under the [Act No. 78/2019](#) on the Security of Network and Information Systems of Critical Infrastructure, or any legislation replacing it. The minister maintains a public register of these operators and publishes it in Section B of the Official Gazette (Stjórnartíðindi). Whether an applicant is an operator of essential services can be verified in [Notice No. 691/2026 on the register of operators of essential services](#), or any subsequent notice replacing it. The register in force at the close of the application deadline applies.

5.6 Award decision

The expert panel evaluates the applications and submits to the Eyvör Board a reasoned evaluation and an advisory ranking of applications based on the expert evaluation. The chair of the expert panel presents the results of the evaluation to the Eyvör Board. The Board decides on the grant awards based on the expert panel's evaluation and the available documents and subsequently submits a proposal to the Minister of Infrastructure, who confirms the allocation of funding.

5.7 Notification of results

Once the award decision has been made, applicants receive a response letter together with the expert panel's evaluation. Notification of the outcome is sent to all applicants, and information on the grants awarded is published on the Eyvör and Rannís websites. Decisions on the award of grants from the Eyvör Cybersecurity Grant are final at the administrative level.

Comments or enquiries from applicants regarding the expert panel's evaluation after the award shall be directed to the Cybersecurity Grant programme officer at Rannís.

³ A survey conducted by Eyvör on the state of cybersecurity among public bodies and companies in Iceland indicated a need to strengthen staff capacity to identify, assess and respond to risks related to the use of artificial intelligence.

⁴ See the [Act on the Security of Network and Information Systems of Critical Infrastructure](#).

6. Grant agreement and payments

6.1 Grant agreement preparation

Rannís prepares the grant agreement with the grantee on behalf of Eyvör. The agreement sets out the rights and obligations of the parties, payment arrangements, conditions for the grant, monitoring and reporting, as well as provisions on non-compliance and recovery. The approved application forms part of the agreement. The agreement also sets out the grantee's obligation to report changes in ownership or control, see Section 2.6.

6.2 Payments

Cybersecurity Grant payments are made as follows:

- **80%** of the grant amount is paid after the agreement has been signed.
- **20%** (the balance) is paid after the final report has been approved and the other conditions of the agreement have been met; see Chapter 7 for details. For projects receiving a grant of ISK 12,000,000 or more, a progress report is also required.

6.3 Changes to the project

If changes to the work plan, budget or partners are needed, the project manager shall consult the Cybersecurity Grant programme officer. Changes to individual cost items exceeding 20% of the amount of the cost item concerned in the approved budget are subject to prior approval by the Cybersecurity Grant programme officer. If such changes are made without prior approval, there is a risk that support for the project will be withdrawn in part or in full and that repayment will be required.

6.4 Publication and dissemination of results

The Cybersecurity Grant is co-funded by the European Union, and grantees are required to hold a presentation in September 2027 at which the main results of the project are presented. All presentation, publication and dissemination of the project's results must state that the project is co-funded by the European Union and supported by Eyvör.

The Eyvör Cybersecurity Grant logo must be used; it can be found on the [grant's website](#) and on the [Eyvör website](#). The EU emblem, together with further guidance on its use, can be found at: [eu-emblem-rules_en.pdf \(europa.eu\)](#).



Co-funded by
the European Union



EYVÖR | NCC-IS

ICELAND CYBERSECURITY
COORDINATION CENTRE



6.5 Ownership of results

The general rule is that ownership and user rights follow each party's contribution. If support is withdrawn due to non-compliance, Eyvör NCC-IS acquires all results that have been delivered to it and may publish them without restriction. Participants in collaborative projects shall conclude an agreement among themselves on ownership and user rights; a draft of such an agreement is available from the Cybersecurity Grant programme officer. If there is any doubt about ownership or user rights, or if the project results involve patentable inventions, trade secrets or third-party intellectual property rights, such matters must be examined specifically and negotiated separately before the agreement is concluded. Such special provisions of the agreement take precedence over the general rule in this section.

7. Monitoring and final reporting

7.1 Project manager

The project manager is the main contact person for Rannís and is responsible for communication concerning the implementation and financial closure of the project. The project manager must have an overview of the total project cost and ensure that each participant keeps separate cost accounts for costs funded by the Cybersecurity Grant. On behalf of Eyvör and under the mandate of the Eyvör Board, Rannís staff are responsible for project monitoring and grant payments and may request access to accounting records to verify costs.

The project manager, the managing director or the board of the company/institution may give notice that a new person will take over as project manager. In the case of a collaborative project, all co-applicants must confirm the new project manager, and this notification must be sent to Rannís for confirmation. The final decision on a change of project manager is subject to approval by Rannís staff.

7.2 Progress report

For projects receiving a grant of ISK 12,000,000 or more, a progress report must be submitted no later than 1 May 2027. Submission of the progress report is a condition for the final payment.

7.3 Final report

The project's final report must be submitted no later than **20 August 2027**, although it may be submitted earlier if the scope of the project warrants it. The final report must be completed and submitted electronically via [My Pages on the Rannís portal](#). The report must describe the progress of the project and, where applicable, any deviations from the original plan. The report must be accompanied by a general ledger transaction listing and an itemised cost statement from the accounts. All costs incurred in connection with the project must be specified in the final report. Once the final report has been approved, no further costs can be claimed for the project. Before the final grant payment is made, a cost audit of the project may be carried out, which may affect the final grant amount.

7.4 Non-compliance, cancellation and recovery

In the event of material non-compliance with the conditions of the grant or the agreement, Eyvör may, following an appropriate procedure, decide to cancel the unpaid part of the grant and/or demand repayment of grant funds already paid. The same applies if the grantee no longer meets the ownership and control conditions, see Section 2.6.

7.5 Further information

The Cybersecurity Grant programme officer at Rannís provides further information and assistance on weekdays from 9:00 to 15:00 on tel. +354 515 5832. General enquiries about the grant, as well as about applications under evaluation, may also be sent to: ncc@rannis.is.