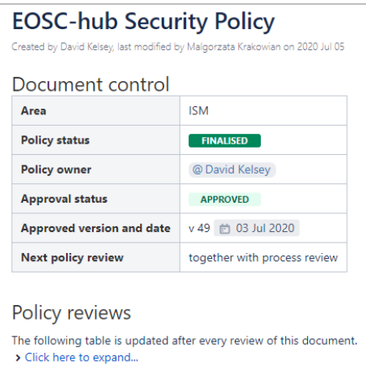
EGI	EOSC-hub	AARC PDK	UK IRIS
https://wiki.egi.eu/wiki/SPG:Documents	https://wiki.eosc-hub.eu/display/EOSC/ISM+Policies	https://aarc-community.org/policies/policy-development-kit/	https://drive.google.com/drive/folders/12YIxNy4ax8_he-jAYUz-N8jHJcdJ_sbB?usp=sharing
The e-Infrastructure Security Policy This policy is effective from 01/02/2017 and replaces an earlier version of this document [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set.		**Top Level Infrastructure Policy Template** This policy is effective from <insert date>.	**UK IRIS Infrastructure Security Policy** This policy, the UK IRIS Infrastructure Security Policy, is effective from <insert date>.
Introduction and Definitions To fulfil its mission, it is necessary for the *e-Infrastructure* to protect its assets. This document presents the *policy* regulating those activities of *participants* related to the security of the *e-Infrastructure*.	**Introduction** To fulfil its mission, it is necessary for the EOSC-hub project and its Collaborating Infrastructures, hereafter jointly called the "Collaborating Infrastructures", to protect their assets. This document presents the policy regulating those activities of participants related to the security of the Collaborating Infrastructures. This security policy is aimed to be compliant with WISE Security for Collaborating Infrastructures (SCI) version 2[R1].	**INTRODUCTION AND DEFINITIONS** To fulfil its mission, it is necessary for the Infrastructure to protect its assets. This document presents the *policy* regulating those activities of *participants* related to the security of the Infrastructure.	**Introduction** To fulfil its mission, it is necessary for the IRIS Infrastructure (https://www.iris.ac.uk) to be protected from damage, disruption and unauthorised use. This document presents the policy regulating those activities of IRIS Participants related to the security of the IRIS Infrastructure.
Definitions	**Definitions**	**Definitions**	**Definitions**
The phrase *e-Infrastructure* when italicised in this document, means all of the people and organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support IT *services*.	The words Collaborating Infrastructure when italicised in this document, means all of the people and organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support the Services.	***Infrastructure*** All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support *services*.	**IRIS Infrastructure** - All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support IRIS Services.
The other italicised words used in this document are defined as follows:	The other italicised words used in this document are defined as follows:		
Policy is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.	*Policy* is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.		
A *participant* is any entity providing, using, managing, operating, supporting or coordinating one or more IT *service(s)*.	A *participant* is any entity providing, using, managing, operating, hosting, supporting or coordinating one or more service(s).	***Participant*** An entity providing, using, managing, operating, supporting or coordinating one or more *service(s).*	**IRIS Participant** - An entity providing, using, managing, operating, supporting or coordinating one or more IRIS service(s).
A *service* is any computing or software system, which provides access to, information about or controls *resources*.	A *service* is any computing or software system accessible by Users of the Collaborating Infrastructures.	***Service*** An *infrastructure* component fulfilling a need of the *users*, such as computing, storage, networking or software systems.	**IRIS Service** - An infrastructure component fulfilling a need of the IRIS Users, such as computing, storage, networking or software systems.
A *resource* is the *equipment* and *software* required to run a *service* on the *e-Infrastructure*, and any *data* held on the *service*.			

EGI	EOSC-hub	AARC PDK	UK IRIS
Included in the definition of *equipment* are processors and associated disks, tapes and other peripherals, storage systems and storage media, networking components and interconnecting media. Included in the definition of *software* are operating systems, utilities, compilers and other general purpose applications, any software required to operate any *equipment*, software and middleware released and/or distributed by the *e-Infrastructure* and any software required to support any application associated with *User Communities* or other authorised *Users*. Included in the definition of *data* are data required to operate any *equipment* defined as a *resource*, data required to operate any *service*, data intended to be processed or produced by any *software* defined as a *resource*, and any application data.			
The *Management* is the collection of the various boards, committees, groups and individuals mandated to oversee and control the *e-Infrastructure*.	The Management is the collection of the various boards, committees, groups and individuals mandated to oversee and control the Collaborating Infrastructures.	***Management*** The collection of the various boards, committees, groups and individuals mandated to oversee and control the Infrastructure.	**IRIS Management** - The collection of boards, committees, groups and individuals mandated to oversee and control the IRIS Infrastructure.
A *User* is an individual who has been given authority to access and use *e-Infrastructure resources*.	A User is an individual who has been given authority to access and use one or more Services and Infrastructure resources.	***User*** An individual or an organisation authorised to access and use *services.*	**IRIS User** - A member of an IRIS Community authorised to access and use IRIS Services by virtue of their ownership of an account on the IRIS Infrastructure Identity and Access Management service [R1].
A *User Community* is a grouping of *Users* and optionally *resources*, usually not bound to a single institution, which, by reason of their common membership and in sharing a common goal, are given authority to use a set of *resources*. Included in the definition of a *User Community* are cases where *resources* are offered to individual *Users* who are not members of an explicitly organised *User Community*.	A User Community is a grouping of Users, usually not bound to a single institution, which, by reason of their common membership and in sharing a common goal, are given authority to use a set of services. Included in the definition of a User Community are cases where services are offered to individual Users who are not members of an explicitly organised User Community.	***Community*** A group of *users*, organised with a common purpose, and jointly granted access to the *infrastructure*. It may act as the interface between individual *users* and the *infrastructure*.	**IRIS Community** - A group of individuals (members), organised with a common purpose, and jointly granted access to the IRIS infrastructure. An IRIS Community may act as the interface between individual members and the IRIS Infrastructure.
The *User Community Management* is the collection of various individuals and groups mandated to oversee and control a *User Community*.	The User Community Management is the collection of various individuals and groups mandated to oversee and control a User Community.		
A *Resource Centre* is an entity having administrative control of *resources* provided to the *e-Infrastructure*. This may be at one physical location or spread across multiple physical locations.		***Service Provider*** An entity responsible for the management, deployment, operation and security of a *service.*	**IRIS Service Provider** - An entity responsible for the management, deployment, operation and security of an IRIS service.
Resource Centre Management is the collection of various individuals and groups mandated to oversee and control a *Resource Centre*.			
		Security Contact A group or individual responsible for operational security of the Infrastructure.	**IRIS Security Officer**- An individual, appointed by the IRIS Management, responsible for operational security of the IRIS Infrastructure.
Other terms are defined in the Glossary [R3].	Other terms are defined in the Glossary [R2].		

EGI	EOSC-hub	AARC PDK	UK IRIS
In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119 [R4]	In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119 [R3]	In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119 2.2	In this document the key words 'must', 'must not', 'required', 'shall', 'shall not', 'should', 'should not', 'recommended', 'may', and 'optional' are to be interpreted as described in RFC 2119 [R2]
Objectives This *policy* gives authority for actions which may be carried out by designated individuals and organisations and places responsibilities on all *participants*.	**Objectives** This policy gives authority for actions which may be carried out by designated individuals and organisations, and places responsibilities on all participants.	**Objectives** This *policy* gives authority for actions which may be carried out by designated individuals and organisations and places responsibilities on all *participants*.	**Objectives** To reduce the likelihood of and impact from security incidents on the IRIS Infrastructure, its Participants and the wider Research community, this policy gives authority for actions to be taken by designated individuals and organisations and places responsibilities on IRIS Participants.
Scope This *policy* applies to all *participants*. Every *Resource Centre* participating in the *e-Infrastructure* autonomously follows their local policies with respect to the *services* and *resources* they own, including those which are part of the *e-Infrastructure*. This *policy* augments local policies by setting out additional *e-Infrastructure*-specific requirements.	**Scope** This policy applies to all participants involved in providing, using, managing, operating, hosting, supporting or coordinating one or more EOSC-hub registered Hub Service(s), hereafter called the "Services". This policy augments local Service policies by setting out additional EOSC-hub and Collaborating Infrastructure specific requirements.	**Scope** This *policy* applies to all *participants*. This *policy* augments local *Service* policies by setting out additional Infrastructure specific requirements.	**Scope** This policy applies to all IRIS Participants. This policy augments IRIS Service Providers' local security policies by setting out additional IRIS Infrastructure specific requirements.
Additional Policy Documents Additional policy documents required for a proper implementation of this *policy* may be found at a location specific to the *e-Infrastructure* [R2]	**Additional Policy Documents** Additional policy documents required for a proper implementation of this policy are to be found in [R4].	**Additional Policy Documents** Additional policy documents required for a proper implementation of this *policy* are to be found at [R1].	
Approval and Maintenance This *policy* is prepared and maintained by the Security Policy Group, approved by the *Management* and thereby endorsed and adopted by the *e-Infrastructure* as a whole. This *policy* will be revised by the Security Policy Group as required and resubmitted for formal approval and adoption whenever significant changes are needed. The most recently approved version of this document is available at a location specific to the *e-Infrastructure* [R2].		**Approval and Maintenance** This *policy* is approved by the *Management* and thereby endorsed and adopted by the Infrastructure as a whole. This *policy* will be maintained and revised by a body appointed by the *Management* as required and resubmitted for formal approval and adoption whenever significant changes are needed. The most recently approved version of this document is available at a location specific to the Infrastructure [R1].	**Approval and Maintenance** This policy is approved by IRIS Management and thereby endorsed and adopted by the IRIS Infrastructure as a whole. This policy will be maintained and revised by a body appointed by the IRIS Management as required and resubmitted for formal approval and adoption whenever significant changes are needed. The most recently approved version of this document is available at [R3].
	EOSC-hub Security Policy Statements		
Roles and Responsibilities This section defines the roles and responsibilities of *participants*.	**ROLES AND RESPONSIBILITIES** This section defines the roles and responsibilities of participants.		
The Management The *Management* provides, through the adoption of this *policy* and through its representations on the various management bodies of the *e-Infrastructure*, the overall authority for the decisions and actions resulting from this *policy* including procedures for the resolution of disputes. The *Management* provides the capabilities for meeting its responsibilities with respect to this *policy*.	**The EOSC-hub Management** The management of the EOSC-hub project includes the Activity Management Board (AMB). Collaborating Infrastructures have their own management structures. Collectively these are all referred to as The Management. The Management provides the overall authority for the decisions and actions resulting from this policy including procedures for the resolution of disputes.	**ROLES AND RESPONSIBILITIES OF THE MANAGEMENT** The *Management* provides, through the adoption of this *policy* and through its representations on the various management bodies of the Infrastructure, the overall authority for the decisions and actions resulting from this *policy* including procedures for the resolution of disputes. The Management maintains the set of policies approved for use within the Infrastructure and ensures that participants are aware of their roles responsibilities. The approved policy	**Responsibilities of the IRIS Management** The IRIS Management provides, through the adoption of this policy and through its representations on the various management bodies of the IRIS Infrastructure, the overall authority for the decisions and actions resulting from this policy including procedures for the resolution of disputes. The IRIS Management maintains the set of policies approved for use within the IRIS Infrastructure and ensures that IRIS Participants are aware of their roles and responsibilities.

EGI	EOSC-hub	AARC PDK	UK IRIS
The *Management* is responsible for ensuring compliance of its *participants* and can represent them towards third parties with respect to this *policy*.	The Management is responsible for providing and maintaining a Privacy Notice for EOSC-hub.	set must meet the requirements of the Snctfi framework [R2].	The IRIS Management must appoint the IRIS Security Officer.
The e-Infrastructure Security Officer and the CSIRT The *Management* must appoint a Security Officer who leads and coordinates the operational security capability (CSIRT). The Security Officer may, in consultation with the CSIRT, the *Management* and other appropriate persons, require actions by *participants* as are deemed necessary to protect the *e-Infrastructure* from or contain the spread of IT security incidents. The Security Officer also handles requests for exceptions to this *policy* as described in section 0.	**The Collaborating Infrastructure Security Officers** The Security Officers from EGI and EUDAT jointly coordinate the operational security capabilities of the project, including the implementation of the Sirtfi framework [R5] by the Collaborating infrastructures. The Security Officers may, in consultation with the Management and other appropriate persons, require actions by participants as are deemed necessary to protect the Collaborating Infrastructures from, or contain the spread of, IT security incidents. The Security Officers handle requests for exceptions to this policy as described below. The Security Officers are responsible for establishing and periodically testing a communications flow for use in security incidents.	**ROLES AND RESPONSIBILITIES OF THE SECURITY CONTACT** The Security Contact coordinates the operational security capabilities of the Infrastructure, including the enabling of compliance with the Sirtfi framework [R6]. The Security Contact may, in consultation with the Management and other appropriate persons, require actions by participants as are deemed necessary to protect the Infrastructure from or contain the spread of IT security incidents. The Security Contact handles requests for exceptions to this policy as described below. The Security Contact is responsible for establishing and periodically testing a communications flow for use in security incidents.	**Responsibilities of the IRIS Security Officer** The IRIS Security Officer coordinates the operational security capabilities of the IRIS Infrastructure, including the enabling of compliance with the Sirtfi framework [R4]. The IRIS Security Officer may, in consultation with IRIS Management and other appropriate persons, require actions by IRIS Participants as are deemed necessary to protect the IRIS Infrastructure from or contain the spread of IT security incidents. The IRIS Security Officer handles requests for exceptions to this policy as described below. The Security Officer is responsible for establishing and periodically testing a communications flow for use in security incidents. The IRIS Security Officer may delegate responsibilities to designated individuals or groups as necessary to provide operational coverage.
User Community Management The *User Community Management* must designate a Security contact point (person or team) that is willing and able to collaborate with affected *participants* in the management of security incidents. The *User Community Management* should abide by the *e-Infrastructure* policies in the areas of Acceptable Use, User Registration and Membership Management and all other applicable policies [R2]. Exceptions to this must be handled as in section 0. They must ensure that only individuals who have agreed to abide by the *e-Infrastructure* AUP [R2] and the *User Community* AUP are registered as members of the *User Community*. *User Community Management* and *Users* that provide and/or operate *resources* or *services* must abide by the Service Operations Security Policy, the Traceability and Logging Policy and all other applicable policies [R2]. For *services* requiring authentication of entities the *User Community Management* must abide by the policy on Acceptable Authentication Assurance [R2]. *User Community Management* is responsible for promptly investigating reports of *Users* failing to comply with the policies and for taking appropriate action to limit the risk to the *e-Infrastructure* and ensure compliance in the future, as defined in section 0.			**Responsibilities of IRIS Communities** IRIS Communities must collaborate with the IRIS Security Officer to proactively limit risk posed to IRIS from their use of the Infrastructure, including the reporting and resolution of suspected or confirmed security incidents and issues arising from Community members' use of the Infrastructure.. IRIS Communities must manage the lifecycle of their members (registration, renewal and removal) to ensure that membership is restricted to only bonafide individuals, and all members are aware of their responsibilities through their acceptance of the IRIS Infrastructure Acceptable Use Policy.
Users *Users* must accept and agree to abide by the *e-Infrastructure* Acceptable Use Policy [R2] and the *User Community* AUP			**Responsibilities of IRIS Users** IRIS Users must abide by the terms of the IRIS Infrastructure Acceptable Use Policy (AUP)[R3]. They must confirm their

EGI	EOSC-hub	AARC PDK	UK IRIS
when they register or renew their registration with a *User Community*. *Users* must use *services* and *resources* only in pursuit of the legitimate purposes of their *User Community*. They must respect the autonomy and privacy of the host *Resource Centres* on whose *resources* it may run. They must not attempt to circumvent any restrictions on access to *resources* and *services*. *Users* must show responsibility, consideration and respect towards other *participants* in the demands they place on the *e-Infrastructure*. *Users* that provide and/or operate *resources* or *services* must abide by the Service Operations Security Policy and all other applicable policies [R2]. For *services* requiring authentication of entities the *Users* must abide by the policy on Acceptable Authentication Assurance [R2]. *Users* may be held responsible for all actions taken using their credentials, whether carried out personally or not. No intentional sharing of *User* credentials is permitted.			acceptance of this AUP when they register or renew their registration with an IRIS Community, and must collaborate in timely reporting and resolution of security incidents affecting the IRIS Infrastructure.
Resource Centre Management The *Resource Centre Management* must designate a Security contact point (person or team) that is willing and able to collaborate with affected *participants* in the management of security incidents and to take prompt action as necessary to safeguard *services* and *resources* during an incident. *Resource Centres* must abide by the Service Operations Security Policy, the Traceability and Logging Policy and all other applicable policies [R2]. *Resource Centres* acknowledge that participating in the *e-Infrastructure* and allowing related inbound and outbound network traffic increases their IT security risk. *Resource Centres* are responsible for accepting or mitigating this risk. *Resource Centres* must deploy effective security controls to protect the confidentiality, integrity and availability of their *services* and *resources*. For *services* requiring authentication of entities the *Resource Centre* must abide by the policy on Acceptable Authentication Assurance [R2].	**Service Management** The Service must designate a Security contact point (person or team) that is willing and able to collaborate with affected participants in the management of security incidents and to take prompt action as necessary to safeguard services and resources during an incident. Services must abide by the Infrastructure Services Security Operations Policy [R4] and the Sirtfi framework [R5]. Services acknowledge that participating in the Infrastructure and allowing related inbound and outbound network traffic increases their IT security risk. Services are responsible for accepting or mitigating this risk. Services must produce and maintain a list of their information assets. They must identify threats to their Service and assets and must perform regular security risk assessments. To mitigate the identified risks Services must deploy effective security controls to protect the confidentiality, integrity and availability of their services and resources. For Services processing personal data, a Privacy Notice must be made available to the Management for the registry of Privacy Notices and presented to Users before or upon first access to the Service.		**Responsibilities of IRIS Service Providers** Service providers must deploy security controls to protect the confidentiality, integrity and availability of their services and designate a security contact to collaborate with the IRIS Security Officer and affected IRIS Participants in the handling of security incidents. The security contact for the service provider shall promptly inform the IRIS Security Officer of any suspected or confirmed security incident that could impact IRIS.
Physical Security All the requirements for the physical security of *resources* are expected to be adequately covered by each *Resource Centre's* local security policies and practices. These should,	**PHYSICAL SECURITY** All the requirements for the physical security of the equipment used to provide a Service are expected to be adequately covered by each Service's local security policies	**PHYSICAL SECURITY** All the requirements for the physical security of resources are expected to be adequately covered by each *Service's* local security policies and practices. These should, as a	**Physical and Network Security** All the requirements for the physical and network security of IRIS Services are expected to be adequately covered by each

EGI	EOSC-hub	AARC PDK	UK IRIS
as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for *equipment* used to provide certain critical *services* such as *User Community* membership services or credential repositories. The technical details of such additional requirements are contained in the procedures for operating and approving such services.	and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for equipment used to provide certain critical services such as User Community membership services, Identity Management Proxies, or credential repositories.	minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for equipment used to provide certain critical services such as *Community* membership services, the Authentication Proxy, or credential repositories.	IRIS Service Provider's local security policies and practices. To support specific IRIS Community workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the IRIS Service to accept or mitigate the risks associated with such traffic.
Network Security All the requirements for the networking security of *resources* are expected to be adequately covered by each *Resource Centre's* local security policies and practices. To support specific *User Community* workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the *Resource Centre* to accept or mitigate the risks associated with such traffic.	**NETWORK SECURITY** All the requirements for the networking security of Services are expected to be adequately covered by each Service's local security policies and practices. To support specific User Community workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the Service to assess and appropriately mitigate the risks associated with such traffic.	**NETWORK SECURITY** All the requirements for the networking security of resources are expected to be adequately covered by each *Service's* local security policies and practices. To support specific *Community* workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the *Service* to accept or mitigate the risks associated with such traffic.	*(see Physical and Network Security above)*
Exceptions to Compliance Wherever possible, *e-Infrastructure* policies and procedures are designed to apply uniformly to all participants. If this is not possible, for example due to legal or contractual obligations, exceptions may be made. Such exceptions should be time-limited and must be documented and authorised by the e-Infrastructure Security Officer and, if required, approved at the appropriate level of the Management. In exceptional circumstances it may be necessary for *participants* to take emergency action in response to some unforeseen situation which may violate some aspect of this *policy* for the greater good of pursuing or preserving legitimate *e-Infrastructure* objectives. If such a *policy* violation is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level of the *Management* commensurate with taking the emergency action promptly, and the details notified to the *e-Infrastructure* Security Officer at the earliest opportunity.	**EXCEPTIONS TO COMPLIANCE** Wherever possible, Infrastructure policies and procedures are designed to apply uniformly to all participants. If this is not possible, for example due to legal or contractual obligations or due to compelling operational difficulties, exceptions may be made. Such exceptions should be time-limited and must be documented and authorised by an Infrastructure Security Officer and, if required, approved at the appropriate level of the Management. Such exceptions must not unduly compromise the integrity or trustworthiness of the Infrastructure. In exceptional circumstances it may be necessary for participants to take emergency action in response to some unforeseen situation which may violate some aspect of this policy for the greater good of pursuing or preserving legitimate Infrastructure objectives. If such a policy violation is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level of the Management commensurate with taking the emergency action promptly, and the details notified to the Infrastructure Security Officers at the earliest opportunity.	**EXCEPTIONS TO COMPLIANCE** Where the processes described lead to obvious injustice and hardship due to an implementation of the process being unduly hard, a time-limited and documented exception may be implemented after the explicit approval of Management. Any such exception must be followed by immediate and concrete steps to address the deficiencies created within a limited time period commensurate with the discrepancy induced. The invocation of the hardship clause must not compromise the integrity or trustworthiness of the Infrastructure.	**Exceptions to Compliance** Wherever possible, IRIS Infrastructure policies and procedures are designed to apply uniformly to all IRIS Participants. If this is not possible, for example due to legal or contractual obligations, exceptions may be made. Such exceptions should be time-limited and must be documented and submitted to the IRIS Infrastructure Security Officer for approval at the appropriate level of the IRIS Management. In exceptional circumstances it may be necessary for IRIS Participants to take emergency action in response to some unforeseen situation which may violate some aspect of this policy. If such an action is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level of local management commensurate with taking the emergency action promptly. Details of the action taken must be notified to the IRIS Security Officer at the earliest opportunity.
Sanctions *Resource Centres* that fail to comply with this *policy* in respect of a *service* they are operating may lose the right to have their *services* recognised by the *e-Infrastructure* until compliance has been satisfactorily demonstrated again. *User Communities* who fail to comply with this *policy* may lose their right of access to and collaboration with the *e-Infrastructure* and may lose the right to have their *services* recognised by the *e-Infrastructure* until compliance has been satisfactorily demonstrated again.	**SANCTIONS** Services that fail to comply with this policy may lose the right to be recognised by the Infrastructure until compliance has been satisfactorily demonstrated again. User Communities who fail to comply with this policy may lose their right of access to and collaboration with the Infrastructure and may lose the right to have their services recognised by the Infrastructure until compliance has been satisfactorily demonstrated again. Users who fail to comply with this policy may lose their right of access to the Infrastructure, and may have their activities	**SANCTIONS** *Services* and Communities that fail to comply with this policy may lose their rights and benefits until compliance has been satisfactorily demonstrated again. Any activities thought to be illegal may be reported to appropriate law enforcement agencies.	**Sanctions** IRIS Service Providers that fail to comply with this policy in respect of a service they are operating may lose the right to have their services recognised by the IRIS Infrastructure until compliance has once more been satisfactorily demonstrated. IRIS Communities who fail to comply with this policy may lose their members' right of access to and collaboration with the IRIS Infrastructure, and may lose the right to have their services recognised by the IRIS Infrastructure until

EGI	EOSC-hub	AARC PDK	UK IRIS
Users who fail to comply with this *policy* may lose their right of access to the *e-Infrastructure*, and may have their activities reported to their *User Community* or their home organisation. Any activities thought to be illegal may be reported to appropriate law enforcement agencies.	reported to their User Community or their home organisation. Any activities thought to be illegal may be reported to appropriate law enforcement agencies.		compliance has once more been satisfactorily demonstrated. IRIS Users who fail to comply with this policy may lose their right of access to the IRIS Infrastructure, and may have their activities reported to their IRIS Community or their home organisation. Any activities thought to be illegal may be reported to appropriate law enforcement agencies.
			Further Information and Guidance The current version of this policy and additional documents, together with guidance for implementation of IRIS security policy, may be found at [R3].
References **R 1**-(Old version) Grid Security Policy https://documents.egi.eu/document/86 **R 2**-Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents **R 3**-EGI Glossary. http://www.egi.eu/about/glossary/ SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71 **R 4**-Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997. http://www.rfc-editor.org/info/rfc2119	**REFERENCES** R1WISE Security for Collaborating Infrastructures SCI V2 (31 May 2017) https://wise-community.org/sci/ R2 EOSC-hub Glossary https://confluence.egi.eu/display/EOSC/EOSC-hub+Glossary R3 IETF RFC2119 https://www.ietf.org/rfc/rfc2119.txt R4 ISM Policies EOSC-hub Security Policy EOSC-hub Service Operations Security Policy EOSC-hub Acceptable Use Policy and Conditions of Use https://confluence.egi.eu/display/EOSC/ISM+Policies https://confluence.egi.eu/display/EOSC/EOSC-hub+Security+Policy https://confluence.egi.eu/display/EOSC/EOSC-hub+Service+Operations+Security+Policy https://confluence.egi.eu/display/EOSC/EOSC-hub+Acceptable+Use+Policy+and+Conditions+of+Use R5 The Security Incident Response Trust Framework for Federated Identity (Sirtfi) version 1.0 https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf	[R1] <Insert a link to all Infrastructure policies> [R2] https://www.igtf.net/snctfi/	**References** [R1] https://iris-iam.stfc.ac.uk [R2] https://tools.ietf.org/html/rfc2119 [R3] https://iris.ac.uk/security [tbd] [R4] https://refeds.org/sirtfi

EGI	EOSC-hub	AARC PDK	UK IRIS
	EGI.eu, licensed under a Creative Commons Attribution 4.0 International License. https://documents.egi.eu/document/3015 Other Sources / Attribution / Acknowledgements: SCI version 2 from the WISE Community, used under CC BY-NC-SA 4.0.	used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).	European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Other Sources / Attribution / Acknowledgements: "EGI Top Level Security Policy", used under CC BY-NC-SA 4.0.The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).
Cells / Words *80 / 1723*	*Cells / Words* *76 / 1204*	*Cells / Words* *46 / 797*	*Cells / Words* *56 / 1180*