Community Operations Security Policy

1 Introduction

This policy is effective from May 20 2019]. This policy is one of a set of documents that together define the Security Policy [1] and must be considered in conjunction with all the policy documents in the set.

The purpose of this policy is to ensure that the Community's use of the Infrastructure is appropriate, and that the Infrastructure and Communities will respond together to accidental or malicious use that is excessive, harmful to others, or not for appropriate purposes.

This policy applies to the Community Manager and other designated Community management personnel. It places requirements on Communities and it governs their relationships with all Infrastructures with which they have a usage agreement. The Community management personnel must ensure awareness and acceptance, by the Community and its Users, of the responsibilities documented in this Policy.

2 Definitions

A Community is a set of one or more groups of persons (Users), organised with a common purpose, with a Community Management willing to take responsibility for all sub-groups, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, Communities authorised to use particular portals or gateways, and geographically organised communities.

3 Community Operations Security Policy

By participating in the Infrastructure, a Community Manager agrees to the conditions laid down in this document and other referenced documents which may be revised from time to time.

1. *The Community must choose a globally unique name that identifies the Community in the Infrastructure. This name shall be based on a URN prefix that is persistently assigned to the Community or a fully-qualified domain name from the global domain name system assigned to the Community, by the relevant naming authority.*
2. *The Community shall provide and maintain, in a repository designated by the Infrastructure, accurate contact information as specified by the Infrastructure. These contacts must include at least two people in a Community management role, and one or more in a security contact role.*
3. *The Community contacts shall be authoritative for management decisions, security actions and operational issues relating to the Community's use of the Infrastructure, and any services operated by or on behalf of the Community that interact with the Infrastructure. They shall respond to enquiries in a timely fashion as defined in the Infrastructure operational procedures, giving priority to security actions.*
4. *The Community must define, and provide to the Infrastructure, a Community Acceptable Use Policy (AUP) as described in the Community Membership Management Policy Template [1], and ensure that its Users are aware of and agree to abide by this AUP.*
5. *The Community shall comply with the Infrastructure Security Policy. The Community shall assess its compliance with this Policy at least once per year, and inform the Infrastructure Security Officer of any violations encountered in the assessment, and correct such violations in a timely manner.*
6. *The Community shall comply with the Infrastructure security incident response policies and procedures and respond promptly to requests from Infrastructure Security Operations.*
7. *The Community shall ensure that a Community membership Registry is provided in compliance with the Community Membership Management Policy. It shall release relevant attributes and assertions to the Infrastructure sufficient to make access control decisions. The real name of the member should be released whenever possible.*

8. *The Community shall ensure that any services operated by or on behalf of the Community that interact with the Infrastructure are operated in compliance with the Service Operations Security Policy.*
9. *The Community shall ensure that information provided by the Infrastructure is only used for administrative, operational, accounting, monitoring and security purposes. The Community shall ensure that due diligence is applied in maintaining the confidentiality of such information.*
10. *The Infrastructure and the Resource Centres may control access to their resources for administrative, operational and security purposes.*
11. *The Community shall apply all reasonable diligence to ensure that its use of any software at a Resource Centre complies with applicable license conditions and the Community shall hold the Resource Centre free and harmless from any liability with respect thereto.*
12. *Any software provided by the Infrastructure is provided on an as-is basis only, and may be subject to its own license conditions. Without prejudice to provisions set forth in more specific agreements, there is no guarantee that any service operated by the Infrastructure is suitable for any particular purpose. In particular, they are not to be used for any purpose which creates the possibility of personal injury, material loss, or the design of safety-critical products and clinical decision support, if they fail or malfunction. The Infrastructure, the Resource Centres and other Communities are not liable for any loss or damage in connection with participation of the Community in the Infrastructure.*

4 References

[1] https://git.scc.kit.edu/m-team/hdf-info/tree/master/policies