Sharing allow: TLP - GREEN	**Approved**

Information Security Glossary

Document ID: **SEC-00**

For: Alliance Federation

Approval Date: 2023-06-07

Approved By: NSC

In the event of a discrepancy between the definitions in this Glossary and those in any other document, the definitions in this Glossary of Terms take precedence.

Alliance Federation Systems and Services:

The technology elements required to implement, operate and manage national services. Not including any elements that have no dependencies with national services.

Data Custodian:

The person who operationally manages one or more sets of data under the direction of the Data Owner or Data Steward.

Data Owner:

The senior-most role accountable for the data throughout its lifecycle.

Data Steward:

The delegate of the ***Data Owner,*** a role that oversees the lifecycle of one or more sets of data associated with a ***National Service***. And can make those decisions as delegated by the ***Data Owner***.

National Service:

Advanced Research Computing (ARC) and/or other related capabilities offered by the Alliance Federation (see service map)

Networking Device

Any computing device either physical or virtual that aids, inhibits, prevents, inspects, or mutates the flow of information between network connected computing devices.

Network Security Zone

A single security domain consisting of services, assets, applications, or data which share the same risk or security profile.

Risk:

Risk is an uncertain event or condition which, if it occurs, affects the ability of an organization to achieve its operational or strategic objectives.

Risk Management:

The planned and systematic approach for the identification, assessment, response and monitoring of risk to maximize opportunities and minimize losses.

Risk Owner:

The role accountable for the effective management of a specific risk or risk category. This is typically an executive or management role that has the authority and accountability to assume risk on behalf of the organization and ensure risks are effectively managed.

Residual Risk:

The risk score after risk treatment has been completed.

Risk Tolerance:

Risk tolerance is how much risk an organization can withstand to achieve its strategic objectives.

Service Owner:

The role accountable for the effective management (including the action required to respond, document, and monitor risks as directed by the Risk Owner) of a specific service, infrastructure, or service portfolio.

Vulnerability:

Weakness in an information system, system security procedures, internal controls, or

implementation that could be exploited or triggered by a threat source.

RACI chart definitions

Accountable (A):

The role is ultimately answerable for the activity or decision to be made.

Responsible (R):

“Responsible” refers to the person or group who actually completes the task – aka “the doer.” There always has to be at least one Responsible per each task.

Consulted (C):

“Consulted” is the adviser for the given task or entire project. Normally, this is the subject matter expert whose opinion you seek before making the final decision or action.

Informed (I):

“Informed” are the people you keep updated on how the process is going. These would be the people who you will notify once the task is completed and who may take action as the result of the outcome. There can be as many “informed” as necessary per process.