



## Jericho Forum™ Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterized future.

Whilst building on “good security”, the commandments specifically address those areas of security that are necessary to deliver a de-perimeterized vision.

The commandments serve as a benchmark by which concepts, solutions, standards, and systems can be assessed and measured.

### Fundamentals

- 1. The scope and level of protection should be specific and appropriate to the asset at risk.**
  - Business demands that security enables business agility and is cost-effective.
  - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.
  - In general, it's easier to protect an asset the closer protection is provided.
- 2. Security mechanisms must be pervasive, simple, scalable, and easy to manage.**
  - Unnecessary complexity is a threat to good security.
  - Coherent security principles are required which span all tiers of the architecture.
  - Security mechanisms must scale; from small objects to large objects.
  - To be both simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms.
- 3. Assume context at your peril.**
  - Security solutions designed for one environment may not be transferable to work in another. Thus, it is important to understand the limitations of any security solution.
  - Problems, limitations, and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

### Surviving in a Hostile World

- 4. Devices and applications must communicate using open, secure protocols.**
  - Security through obscurity is a flawed assumption – secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.
  - The security requirements of confidentiality, integrity, and availability (reliability) should be assessed and built in to protocols as appropriate; not added on.
  - Encrypted encapsulation should only be used when appropriate and does not solve everything.
- 5. All devices must be capable of maintaining their security policy on an un-trusted network.**
  - A “security policy” defines the rules with regard to the protection of the asset.
  - Rules must be complete with respect to an arbitrary context.
  - Any implementation must be capable of surviving on the raw Internet; e.g., will not break on any input.

## The Need for Trust

6. **All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place.**
  - Trust in this context is establishing understanding between contracting parties to conduct a transaction, and the obligations this assigns on each party involved.
  - Trust models must encompass people/organizations and devices/infrastructure.
  - Trust level may vary by location, transaction type, user role, and transactional risk.
7. **Mutual trust assurance levels must be determinable.**
  - Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.
  - Authentication and authorization frameworks must support the trust model.

## Identity, Management, and Federation

8. **Authentication, authorization, and accountability must interoperate/exchange outside of your locus/area of control.**
  - People/systems must be able to manage permissions of resources and rights of users they don't control.
  - There must be capability of trusting an organization, which can authenticate individuals or groups, thus eliminating the need to create separate identities.
  - In principle, only one instance of person/system/identity may exist, but privacy necessitates the support for multiple instances, or one instance with multiple facets.
  - Systems must be able to pass on security credentials/assertions.
  - Multiple loci (areas) of control must be supported.

## Access to Data

9. **Access to data should be controlled by security attributes of the data itself.**
  - Attributes can be held within the data (DRM/metadata) or could be a separate system.
  - Access/security could be implemented by encryption.
  - Some data may have “public, non-confidential” attributes.
  - Access and access rights have a temporal component.
10. **Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.**
  - Permissions, keys, privileges, etc. must ultimately fall under independent control, or there will always be a weakest link at the top of the chain of trust.
  - Administrator access must also be subject to these controls.
11. **By default, data must be appropriately secured when stored, in transit, and in use.**
  - Removing the default must be a conscious act.
  - High security should not be enforced for everything; “appropriate” implies varying levels with potentially some data not secured at all.

## Conclusion

De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness:

- It will happen in your corporate lifetime.
- Therefore, you need to plan for it and should have a roadmap of how to get there.
- The Jericho Forum has a generic roadmap to assist in the planning.