Web & FTP Server Security Policy

Version 2.7

Document version control page

Prepared By

Version	Date	Author	Update Description
1.0	12/06/08	JayaseelanJ	Initial Issue
1.1	22/08/08	JayaseelanJ	Format changes
1.2	10/09/09	JayaseelanJ	Policy Document Reviewed
1.3	12/07/2010	J.Jayaseelan	Policy Document Reviewed
1.4	25/11/2011	Jayaseelan J	Policy Document Reviewed and ISM Name changed to ISH
1.5	27/06/2012	Jayaseelan J	Policy Document Reviewed
1.6	27/06/2013	Jayaseelan J	Policy Document Reviewed
1.7	21/06/2014	Jayaseelan J	Policy Document Reviewed
1.8	01/08/2014	Jayaseelan J	Policy Document Reviewed as per ISO 27001:2013 requirement
1.9	22/06/2015	Jayaseelan J	Policy Document Reviewed
2.0	14/06/2016	Jayaseelan J	Policy Document Reviewed
2.1	15/11/2017	Santhosh S	Policy Document Reviewed
2.2	12/06/2018	Santhosh S	Policy Document Reviewed
2.3	10/07/2019	Santhosh S	Policy Document Reviewed
2.4	09/11/2020	Santhosh S	Policy Document Reviewed
2.5	06/12/2021	Santhosh S	Policy Document Reviewed
2.6	02/12/2022	Santhosh S	Policy Document Reviewed
2.7	05/12/2023	Muthukrishnan B	Policy Document Reviewed

Reviewed and Approved By

Version	Date	Reviewed by	Approved By	Owner
1.0	12/06/08	Mr. Madhavaswamy	Mr. R.Kumar	ISM
1.1	22/08/08	Mr. Madhavaswamy	Mr. R.Kumar	ISM
1.2	10/09/09	HR Director	Mr. R.Kumar	ISM
1.3	13/07/2010	HR Director	Mr. R.Kumar	ISM
1.4	28/11/2011	HR Director	Mr. R.Kumar	ISH

1.5	27/06/2012	HR Director	Mr. R.Kumar	ISH
1.6	28/06/2013	HR Director	Mr. R.Kumar	ISH
1.7	21/06/2014	HR Director	Mr. R.Kumar	ISH
1.8	01/08/2014	HR Director	Mr. R.Kumar	ISH
1.9	22/06/2015	HR Director	Mr. R. Kumar	ISH
2.0	14/06/2016	HR Director	Mr. R .Kumar	ISH
2.1	15/11/2017	HR Director	Mr. R .Kumar	ISH
2.2	12/06/2018	HR Director	Mr. R .Kumar	ISH
2.3	10/07/2019	HR Director	Mr. R .Kumar	ISH
2.4	09/11/2020	HR Director	Mr. R .Kumar	ISH
2.5	06/12/2021	HR Director	Mr. R .Kumar	ISH
2.6	02/12/2022	HR Director	Mr. R .Kumar	ISH
2.7	05/12/2023	HR Director	Mr. R .Kumar	ISH

1. PURPOSE

The Purpose of this policy is to establish standards for the base configuration of any web server that is owned and/or operated by AEL Data. Effective implementation of this policy will streamline the web services of AEL Data.

2. SCOPE

This policy applies to web server(s) & FTP servers owned and/or operated by AEL Data network, and to servers registered under any AEL Data owned network domain.

3. ROLES AND RESPONSIBILITIES

3.1. The designated IT Team shall be responsible for ensuring the implementation of this policy for their respective web servers.
3.2. The administrator shall also coordinate with the Audit Team for required auditing of the server(s).

4. REFERENCE STATEMENTS

4.1. All public web & FTP servers shall be in protected zones (DMZ) with implementation of firewalls and IPSs and high availability solutions.
4.2. Intranet web servers will be accessible to the intranet.
4.3. Access to web & FTP servers shall be restricted physically. Access over Internet shall be restricted to the assigned service only. For any other requirements access shall be authenticated and based on the source IP address.
4.4. Critical information, such as databases, that can be modified shall not be on the web servers where it could be damaged or modified by unauthorized parties. Such information shall be on secure machines that are preferably on a separate LAN segment. Web & FTP Servers shall only provide user access to such information.
4.5. Any application update shall not be on the actual web server but on a staging server. Access methods shall be enabled such that only authorized originating individual or system shall be allowed to perform changes to any available information, even on the staging server.
4.6. Changes and updates to the web pages on the server shall be from the intranet only.
4.7. Formal Change management procedure must e followed before any change is done on the production web & FTP server
4.8. After any changes or updates to the contents of the web pages on the server shall be checked for intentional or unintentional malicious content and virus in the content on the staging server before final change of the production web server pages.
4.9. Only authorized persons, developers or content managers shall establish new pages or make modifications (such as changing layouts, adding links or updating contents) to existing web pages.
4.10. Audit and Log of all activities referring to the operating system, access to the system, and access to web pages shall be maintained and archived. All rejected accesses and services shall be logged and listed in exception reports for further scrutiny.
4.11. All web servers shall synchronize their time to the standard time of the organisation as per the Time Synchronization Policy.
4.12. On restoring form backup, the respective Web & FTP server administrator and the Web contents manager shall check out the contents of each page for correctness for FTP Check the Virtual directory's in Internet information services manager.
4.13. In case a web server page(s) is found to have been defaced, the web server administrator shall be informed immediately,
4.14. Software in development and testing shall be kept strictly separate from production software. This refers to both new software and old software being modified. This policy could be further supported by having separate individuals work in development areas and production areas and by having a physical separation of development and production equipment.
4.15. All web pages should be constantly checked.

4.16. All newly released system software patches, bug fixes and upgrades shall be expediently and regularly reviewed and installed on the web & FTP server as per the Patch Management Policy.

4.17. Before returning a web server that has been defaced back to service, all web pages, system software, and system configuration files shall be thoroughly checked for changes and wherever required the latest backup versions shall be loaded.

4.18. Production web servers shall not be used for Internet browsing, mail reading and for office automation.

4.19. All FTP Login & websites hosted but whose contents are not maintained by AEL Data shall have a prominently displayed Disclaimer that states that AEL Data is not responsible for any discrepancies in the web pages' contents.

4.20. Database backup (incremental) should be taken on a daily basis, and complete backup on a weekly basis, refer to the Backup Policy for more details.

5. COMPLIANCE

5.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.

5.2. Audits will be managed in accordance with the Information Security Audit Procedure.

5.3. Every effort will be made to prevent audits from causing operational failures or disruptions.

6. EXCLUSIONS

There are no exclusions to the above guidelines

7. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action as per HR & Admin Procedure.