International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Reliability Management: Setting-up Cloud Server in Higher Education

Salaki Reynaldo Joshua, Tini Mogea

Abstract*: This article shows the reliability plan and reliability manual for setting up two cloud servers for Higher Education. These two servers are used for Primary Operation Services and Standby Operation Services. This reliability plan shows what activities can be performed while setting up servers and at what reliable timings. It also shows the tools and techniques that will be used for designing, analysis and testing services during project development. It has the different management strategies for suppliers and specific standards and policies for setting up a server and for quality assurance and product maintainability. This plan and manual shows how to provide a full backup system of servers and a recovery unit in case of emergencies. This also shows how to setup a security control system, supported by firewalls with adequate warranty

***Keywords*: reliability manual, reliability plan, cloud servers, security system, recovery system.**

I. INTRODUCTION

Higher Education resources is a small group of social media strategists which is planning to include two dedicated cloud servers in their organization [28]. One will be used for Primary Operation Services and other one will be for Standby Operation Services which is mirrored from the primary server. To setup these two servers they are considering to hire Tech company which is a newly medium sized cloud service provider. They need Tech company to assist them in managing the hosting and operation of their web-based systems. They require a plan for two full dedicated cloud servers and a fully back-up system for this setup. In addition to that they also require a plan for "Disaster Recovery Unit" supported by several machines within Higher Education premises which will help them to recover data in case of emergencies. Security is a major concern for Higher Education so they also require a full security system plan. They require them to assist in setting up a Security Control System supported primarily by firewalls. This mentioned information system infrastructure must be supported with some adequate warranties. Higher Education insist the availability of a system is paramount.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Salaki Reynaldo Joshua*, Informatics Engineering, Universitas Sam Ratulangi, Manado, Indonesia, Email: salakirjoshua@unsrat.ac.id
Tini Mogea, English Education, Universitas Negeri Manado, Tondano, Indonesia. Email: tinimogea@unima.ac.id

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

So, service legal agreement should be negotiated for the benefit of its clients. In the reliability plan it will show the specific standards for the system. A plan will include different tools and techniques for designing, analyzing, testing and managing system and different dedicated timings for different stages.

Higher Education is of small social media strategists which require Tech company to setup two cloud servers for them where one will be used for "Primary Operation Services" and another one will be used for "Standby Operation Services" which is mirrored from the primary server [23,24,25,26]. Secondly, they require them to establish a 'full backup system' for the above setup. Thirdly they need a "Disaster Recovery Unit" which will be supported by several standard machines within Higher Education premises. Lastly, they require them to setup a "Security Control System" which will be supported primarily by firewalls. The factors affect organizational reliability are Internet connectivity to the servers, stability of the server hardware systems, server software systems, environmental and power stability within the hosting facility. Each of the these needs to be considered when attempting to assure or improve the overall reliability of an organization and their services maintainability.

The main issue is that Higher Education requires a cloud hosting service with security control, back-up system and disaster recovery unit in case of emergencies [10]. To establish this in an organization Tech company needs to go through specific activities and management for a good reliable solution for Higher Education. Reliability is usually affected during design development stage, production quality control, control of suppliers and subcontractors and mainly maintenance [26]. If these activities are handles well then organization will be reliable enough to run a successful business. Tech company needs to form an Engineering Based Organization because knowledge, skills and different techniques will be required from engineering staff to setup a reliable and secure server room for a reliability engineering during safety analysis procedures and maintainability engineering.

To host a social media website, it needs a powerful server of a kind of a user based with optimization of a server within a proper guidelines of Tech company services. Social networking is a site loaded with loads of traffic so it needs a proper analysis of a design, testing, maintenance, reports checking etc [14]. Following we provide with the activates that can be performed to achieve a reliable hosting and services for a social networking site.

a. Design.

A good interface design and well managed website highly effects the website efficiency and effectiveness [2]. This stage should be done at first to accomplish any good IT infrastructure. Design decisions should be made in detail.
Reliability of a product is heavily depending on the decisions made during this process. Good design is derived from and documented by building of different models. Systems design should involve how a system will work, specified in detail while using a technology. Each component of the final solution of a product is heavily influenced by the design of other components. Systems design activities must be done in parallel. All design activities develop a specific portion each for the whole system. The design process must be organized to prevent any failures. Design principles must be used and if any differences occur from the principles, then those must be detected and corrected. Discovery of even few deficiencies at an early stage will save a lot of cost rather than changing the design at later stage which will affect the reliability of a product. The designers must aim to create failure-free designs when manufactured and should be used as specified.

b. Analysis

Analysis of a design and products should be done to prevent any future failures. Failures that have occurred before should be analyzed in detail by an analysis team. Different analysis can be done by a team like physics of failure, finite element analysis (FEA), data analysis, warranty analysis, design review based on failure mode (DRBFM), prediction of reliability etc [27]. If these analyses done properly then it will surely help to achieve a durability and maintainability of a service. Other analysis like detail study on lessons learned on previous programs and experiments on designs. By doing analysis we can also find out the fatigue life of products.

c. Verification and Testing

Activities like verification must be done as well for both software and hardware components to check reliability. Verification include activates like life testing of a software and hardware product [18]. Testing of a quality and control, conjuration control and sub-system level testing. If a problem arises then a problem-solving methods and techniques should be applied to finally verify the product.

d. Configuration Control

This is the process where a design standard can be known and controlled. This applied to both hardware and software. Detailed specifications of a product and component must be identified and changes must be made accordingly for a reliability. Configuration control is important because it helps to identify the

4 International Journal of Electronic Com merce Studies

issue in the software and hardware and it can be controlled through this process [8].

e. Validation

For a reliable network, validation must be done for internal and external factors. Internal factors validation is like validation of a system and requirements and External factors include environmental changed validation which directly influences the system. Validation is necessary for full functioning of a system. This process helps in solving issues in design and manufacturing. Environmental validation helps to see if a system is working and responsive to a that environment [3]. Activities for this process includes like test to failure and test to success. Design validation and a process validation are both important. Design validation includes durability, functional tests, environmental tests and capability of a design. Process validation includes the validation of a working system and it is fully capable of working in a specific environment.

f. Maintenance

Maintenance activity must be conducted in case of failure of a product. Diagnosis of a product should be done for repairing. After repairing, it must be ensured durability and also to prevent future failure, so that the quality product runs in a system [21]. Different maintenance technique must be applied based on the type of product or a component.

g. Reliability Reports Monitoring

IT professionals must monitor individual applications and processes to analyze how much of the available resources is in use. They may use a comprehensive performance analysis on both application impact and overall capacity to help plan for deployment and grow server capacity with the flow demand quantity. Reliability performance checking on a regular basis and reliability reporting helps to track down any performances issues in the application which then generates an alert and report for improvement and further analysis [20]. Proper actions can then be taken to remove any issues. Reliability monitoring measures the whole system and reports on how well a whole system operates and is it performing as expected or not [7] (Microsoft, 2017). Monitoring and reporting is very critical part because if not done and if part of a system stops responding then it affects the reliability. Reports are a great way to analyze data and make changes accordingly. Tools and techniques can be used which generate reports on a regular basis and it then can be monitored by IT professionals. This is an easy way of monitoring and controlling because it saves a lot of time.
Probability of failure on Demand (POFOD). This method must be used to quantify reliability. It calculates probability and statistical figures because for reliability, it's uncertain. For instance, data may show that a power supply will fail at average rate of once per 205 h. So, if 2000 server units are build, and operated for 2000 hours straight, it cannot be said that whether power supply will fail or not but estimated figures can be checked thorough this method within statistical confidence limits because probability failure will lie around probability figure. Following calculation can be used by Tech Company [5].

Table- I: Relevant Research

No	Calculation	Formula
1	Frequency of dangerous undetected failure	λ_{du}
2	Frequency of dangerous detected failure	λ_{dd}

3	Proof Test Interval	T_P
4	Mean Time to Repair	T_R
5	Probability of Failure on Demand (POFOD)	$\lambda_{du} \cdot (T_P/2 + T_R) + \lambda_{dd} \cdot T_R$

II. LITERATURE REVIEW

A. Cloud Computing

Cloud computing is a mechanism, where a bunch of ICT resources are interconnected and almost limitless, both infrastructure and applications are owned and managed entirely by third parties, allowing customers to use these resources on-demand through networks both private and public networks [20]. Users of cloud computing services can access files in real time via the internet without the need to install local computers.

Cloud computing or cloud computing is technology that utilizes internet services using a virtual server center with the purpose of maintaining data and applications [6,9]. The existence of cloud computing will obviously lead to changes in the way information technology systems work in an organization. This is because cloud computing through the concepts of virtualization, standardization and other fundamental features can reduce the costs of Information Technology (IT), simplify management of IT services, and accelerate service delivery. In general, cloud computing architecture consists of (1) Infrastructure as a Service (IaaS) (2) Platform as a Service (PaaS) and (3) Software as a Service (SaaS).

B. Reliability Manual

Standard (Policy) IEEE 1633-2008, this policy provides information which is necessary for application of software reliability measurements for an organization. A company must apply IEEE 1633-2008 standard for quality assurance and software reliability. This practice will help is assessing and predicting the reliability of a software. This practice is recommended to be applied. It helps in building the consistent methods and it has a basic principle for collecting the important data that needs to be assessed [16].

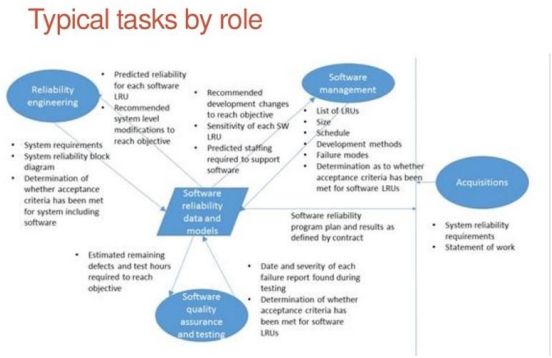

Fig. 1.IEEE Standards 1633-2008 [16]

C. Organization for Reliability

Social Media Strategist must have following responsibilities for an organization reliability [1,4,19]:

1. Designing strategies of social media to achieve marketing targets
2. Creating high quality content.
3. Publishing and managing original content on social platforms.
4. Administering all social media accounts to ensure updated content for everyone.
5. Collaboration with Marketing and Product development teams.
6. Facilitate communication between clients and a company.
7. Must generate weekly or monthly reports on data and performance.
8. Monitor SEO, user engagement and suggest content optimization.
9. Communication with industry professional for a strong network.
10. Training of an internal team members for consistency of new strategies and maintenance of social media strategies.

Web Manager must be fully aware of the hosting solution they have in place. He/she must be aware of site performance and the impact it will have on the user experience. Tools must be used to automatically monitor performance and be use of metrics within a Service Level Agreement.

Service level agreement target must be at following:

1. Availability: The percentage of time when a website is up and running.
2. Reliability: The number of unplanned unavailability or errors that occur on a website.
3. Responsiveness: The speed with which a website responds to traffic.

Web Manager in co-operation with senior management team must select a cloud server that is adequate to support online ambitions and can relate to its performance against metrics like those mentioned above.

System hardening, this process will help in removing any security risks and eliminates any contamination risks. It can be done by removing unnecessary, non-essential user privileges and inactive programs from a system [13]. These programs may provide some useful features to the users but if they have a back-door access to the system then it must be eliminated as soon as possible. Hardening requires any known security weaknesses to be eliminated which creates flaws in a software design and/or in implementation. Steps that should be taken for this process as below:

1. Elimination of any unnecessary software from a system.
2. Remove any unnecessary passwords or usernames.
3. Disable any unnecessary services.
4. Auditing of accounts and privileges must be implemented.
5. Implementation of the least privilege principle for users.
6. Immediate removal of employee accounts who leave the company.
7. Perform weakness tests on the system and a software.

D. Field Return and Warranty Analysis

Field return and warranty data analysis can be extremely useful in identifying any reliability related problems.

Engineering feedback is also important to successful product design and development. The product development process needs to be analyzed to prevent any reliability issues. This task can be accomplished by failure analysis or structured problem solving, or by using a combination of existing continuous improvement tools.

This is useful to determine that a failure occurred due to an assembly problem, software malfunction, electronic or mechanical component failure, corrosion or overheating. Faulty parts must not be used in the new product.

Warranty data must be routinely used for reliability and warranty prediction in new product development. Field failure data of existing products can be used as a reliability predictors of future products than some of the traditional methods, such as reliability growth models or standards-based predictions. Working with warranty data requires an understanding of its specifics and limitations in order to produce meaningful results [17].

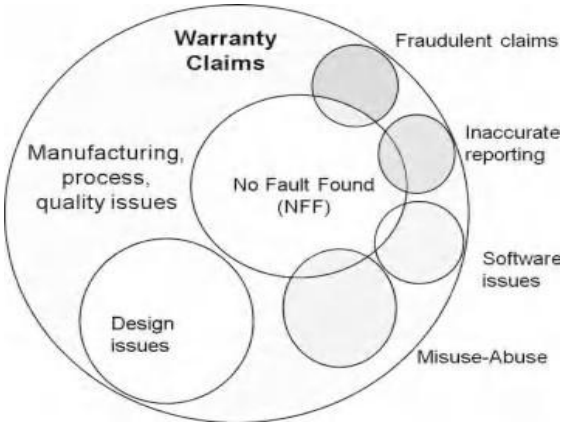

Fig. 2.Warranty Database Content [17]

Figure showed an example of warranty database content. The noise factors include NFF (no fault found) which is very common in the electronics industry, fraudulent claims, inaccurate reporting including missing data and misuse. The amounts of noisy claims would vary significantly based on the type of the product and even individual manufacturer. Therefore, it is very important to clean the data distinguishing between the relevant and irrelevant claims and also further categorize them by failure modes. The product user may also be affected by all product failures. It is sometimes beneficial to process the data without removing those irrelevant claims [12]. High volume warranty analysis helps items to produce and sold continuously, therefore warranty periods for different products begin at different times. It is easier to model warranty in the product age format as opposed to the calendar time format. It is necessary for a reliability professional to remember that warranty periods are usually shorter than the expected life of a product, therefore warranty data does not normally provide enough information to evaluate the reliability at the later phases of product life, where wear and tear is expected.

E. Reliability Test Procedures

Testing for reliability is done to identify any failures and then these can be removed before the system is deployed. Reliability testing should not be applied to prove a single design parameter but should be based on simple key factors and experiments on them which will help in improving reliability [15,22].

a. Integration Stress Testing

Each individual component and entire application should be stressed out with all of its supporting services. This testing contains interactions with other services, processes, and data structures from both internal and external application services. It starts with just basic functional testing. Coded pathways and user scenarios are needed to know. Identify what users are trying to do and identification of the ways, user usually goes through the application. Test scripts should be made. Time of testing should be extended as much as a schedule and budget allows. Testing can also be stretched throughout a month or quarterly or yearly cycle and see how the application functions over a longer period.

b. Use Real-World Testing

A real-world test environment should be used to ensure durability and reliability. Isolated testing may be useful in an early reliability testing process but real-world scenario testing gives you much more real results. It can help in showing some unexpected failures. New application needs to be ensured that it can run in the server space in final configuration with a full experience of n expected customer event profile. It should include running of a new application in the final target environment or as close to the target environment as possible.

III. RESEARCH METHODOLOGY

Figure 3 mentioned activities must be done in a sequence or at a right time to achieve a reliable and durable product. Following is the flow infrastructure of these above activities and if done in this way can help Higher Education to get a reliable cloud servers.

Fig. 3.Research Method

Steps must be taken when collecting data like shown in the diagram below. The goal of Phase A must be to collect meaningful and powerful and usable data on its performance (Figure 4).

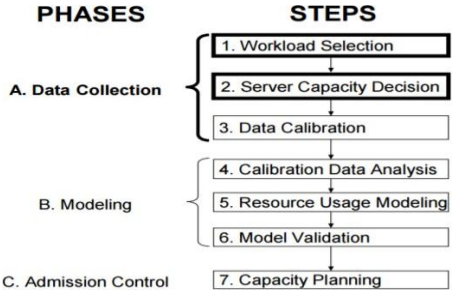

Fig. 4.Reliable Performance Data Collection for Streaming Media Services

Phase A consists of three steps:

1. Identification of a set of disjoint workloads
2. Measuring the server capacity for each pure workload
3. Calibration of the performance statistics

After the data collection phase,

Phase B must be used

1. Careful analysis must be done of the calibrated data which identifies client and server resources and dominating factors that contribute to the measured system saturation.
2. The resource usage model may provide the basis for offline capacity planning.

Phase C for online admission control.

IV. RESULT AND DISCUSSION

All these above-mentioned activities must be done in a sequence or at a right time to achieve a reliable and durable product. Following is the flow infrastructure of these above activities and if done in this way can help Higher Education to get a reliable cloud servers.

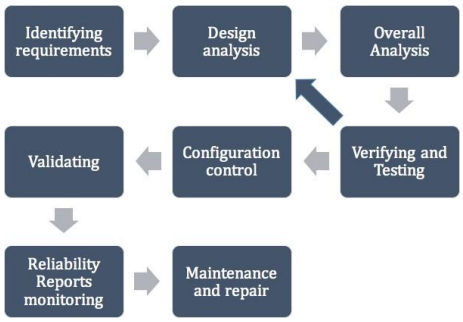

Fig. 5.Research Method

Figure 5 shows steps should be taken in a sequence for a reliable service. Business requirements should be clearly identified before designing a network and planning. Then a design of a network, server should take place according to a website and any suggestion could be made for a better user interface of a website. After a design, a design analysis should be done by a proper team. After design analysis, overall system analysis can be done for further suggestions and improvements on design or system then after doing this next step should be verification of a design and system by testing a hardware and a software by applying different techniques and methods according to the suitable environment. At this stage if a design passes then it can move onto configuration control where a design standard can be known and can be controlled if any excess useless information or component needs to be removed, it can be done at this stage. On the other hand, if a design or a system fails to be successfully verified then it goes back onto design stage and here it can be modified accordingly.

Next step is to validate the product, component or a whole network system. After successful validation by applying different models it then can be installed and run in the system. During running stage different methods and software can be used to generate reports of its performance on a regular basis and these reports then can be monitored and analyzed by IT professionals. And if any performance issues occur here then it can be sent for further repair and maintenance.

These activities will improve organizational abilities like engineering and applications will be consistently of high quality that will have correctness of a system, extensibility and a reliability and everything will be within budget of a company because this way it will ensure cost effectiveness. This will improve processes like reengineering, development, other operations, usage etc. These activities will ensure product quality and continuous process improvement by providing a well-structured and less complex solution. Manageability will be at ease through this infrastructure. Communication between staff members like Higher Education members with Tech company will be at high which will improve effectiveness and efficiency.

Focus on design. Suppliers should focus on design for reliability, operability, maintainability and security. Reliability can be improved from maintenance department if they follow strict rules. Management must design a reliable equipment, must have clear understanding of the operating context. There should also be an involvement from operations and maintenance domain experts, and a project must be led by a member who has professional leadership skills.

Focus on task. Tasks for operating equipment that have started and stopped working and/or handled incorrectly will suffer from higher failure rate. There must be a reliability focused team for tasks and operations who follows strict and enforces specific standard operating procedures.

Focus on maintenance. There must also be a maintenance team who focus on any errors and repair and maintenance procedures. They must focus on maintenance activities and ongoing activities so that they must have an idea of a “mean time between failure (MTBF)”.

Team must work closely with operations and ongoing tasks to ensure that the equipment is always available to produce the required product and meet quality goals to satisfy customer demands. A reliability focused company like Tech Company must work closely with design engineers, procurement specialists and strategic suppliers to improve design for reliability and maintainability, and to avoid the same issues again in future.

Focus on data collection, analysis. Organization must collect, analyse and manage reliability data effectively. Usually reliability starts with a failures modes and effects analysis (FMEA), the reliability blueprint of an operational service or machine. “FMEA” is normally completed by drawing on limited data experience. The FMEA worksheets serves company as a reliability growth management tool. When a team learns something new this way they must modify the FMEA and any number of risks associated with it i.e. risk priority number (RPN).

The organisation must keep on collecting data for maintenance and in operational condition, whether it is working good without any flaws or have any issues. Tools like mathematical reliability engineering and root cause analysis may be used to implement improvement in information and data. Performance monitoring and detailed failure data collection techniques must be used by a team.

Reliability Procedure in Higher Education;

1. Design Procedure.

Setting up a server should not be complicated. IT should be kept simple and well organised. Following are the steps for setting up a server room.

a. Rack-mount equipment

Hardware server and network appliances must not be stacked on a desk or shelf. Such deployment is inexpensive but it causes a big mess which will cause a failure in an organisation. Equipment should not be exposed clearly. Mistakes like coffee spilling, dust getting into an equipment or workers can trip over messy wires easily.

Rack-mount equipment is designed specifically to properly house the server room. It may be pricier but will provide long term benefit and helps from any future damage. It is easier to manage the server room.

There's a server rack for all seasons. The four-post rack designed can be used to hold servers and appliances 19 inches wide. A full height rack typically measures 42U. Other options exist, including desktop variants that range from 5U to 20U.Optional caster wheels can be used for limited mobility and convenience.

b. Isolate servers to reduce noise

There must be a dedicated room for server equipment for a reduction in noise, a small portioned room. A separate room will allow a secure IT equipment against casual theft or tampering.

As Higher Education is a small- medium/medium-big business, where they might not have an option but to place rack in the corner of their room or within the IT department itself, then racks with sound-dampening properties are highly recommended for them for a noise reduction.

c. Server room temperature

A company must have a cooling system in their server room otherwise heat starts to build up quickly which will lead to an equipment failure or it can also shorten its life. It is highly recommended to install one or at least two air-conditioning units in the server room depends on the size of a room.

d. *Wires management*

Proper cable management needs to be done for a durability. Wires must be managed by using an RJ45 patch panel to terminate Ethernet cable runs. The typical patch panel installs in 1U of space and it offers up to 24 ports. It requires a bit of work like stripping a cable, punching it into the patch panel and using a wire tester tool for verification of a successful connection.A professional can be hired here for an installation. A bag of cables must also be tied in one place and releasable ties must be used for this purpose instead of using standard ones.

e. Label everything

Everything in a server room must be labelled properly. Setups must be documented. Labelling will reduce any mistakes done by an employee such as unplugging of wrong wire or restarting without any warning. Label printer must be purchased for this purpose. Servers and network appliances must be labelled with unique descriptive names and their IP addresses. Detailed notes must be written somewhere for an operating instruction relating to networking, data backup or shutting down or starting up of the equipment in some emergencies.

2. Design analysis Procedure

After design, it must be analysed and this can be done by using "Failure Mode Analysis" technique. Following steps should be considered for detailed analysis.

a.Installation of new rack-mounted front-end computer hardware and connect it to Ethernet switches.

b.Installation of IM Server (instant messaging service) software on computer

c.Use of OAM server to add new computer to IM server configuration.

d.Then shut down all front-end and back-end computers in IM server configuration which includes any new computer. This makes services unavailable to users.

e.Then start-up of computers in an order which restores services.

f.Verification of operation of new front-end computer.

g.Reconfiguration of load balancers to distribute traffic to new computer.

This procedure will help in analysing of a server design in growth of hardware components in a server room.

Social media strategist's policy provides a framework for using social media. It is a website where people exchange their information, their opinions and any new experiences that can be learn, develop by other people and also, they have fun on a social media. Employees must be productive while using either a private account or handling a corporate account. The below mentioned policy provides an advice to employees to avoid any issues or any conflicts that might arise in the workplace by careless use of social media. Employees must follow this policy.

This policy covers all the social media content which includes blogging, social networks, status updates and chat rooms. Two elements for employees are considered here like personal account usage at workplace and using company's account.

Table- II: Elements for Employees

No	Using Personal Social Media	Using Company's Account
1	Employees can access their personal social media accounts at work but with a responsibility. We expect them to act responsibly and ensure their productivity is not affected in any manner.	Employees representing company while using a corporate's account must be handled carefully. We expect them to act responsibly and must protect company's image and reputation.
2	Excessive use of social media at work is not allowed. It can reduce efficiency and concentration. Employees may easily get distracted by looking at the available content whether they are using personally or for business.	Employees should be polite, respectful and patient when engaging in conversations on a company's behalf. They should be very careful when making any promises or declarations towards customers and stakeholders.

3	Employees are advised to use an account wisely as it will affect their productivity and this can be seen on their performance reports.	When possible, employees should avoid speaking on matters outside of their field of expertise. They should be careful not to answer any questions or make statements that fall under someone else's responsibility.
4	Statements and comments through personal account usage must not represent any company and others must be ensured of this. We strongly advise to use a disclaimer. For instance, "opinions are my own" to avoid any conflicts and misunderstanding.	Confidentiality policy and Data protection policy must be followed and observe laws on copyright, trademarks, plagiarism and fair use policy must be used. Marketing department must be informed when about to share any major content.
5	Sharing trademarks must be avoided on a personal account without any approval. Confidentiality policies and laws always apply.	Criticism must be handled extra carefully and listen to it calmly. Discriminatory, offensive content must not be posted.
6	Malicious or any offensive content must be avoided towards any person, colleagues or partners. This can cause violation of a company's anti-harassment policy.	Misleading or false content must be removed or corrected as soon as possible.

Disciplinary Consequences, all social media postings are monitored on a corporate account. A disciplinary action will be taken which may lead to termination of an employee if they do not follow this policy's guidelines which includes like disregarding job responsibilities, disclosing any confidential information through any personal or corporate accounts, using offensive comments towards colleagues, partners or members of the online community. Backup and recovery methods are important to data protection and security. Any loss of data due to file corruption, virus, security or human error is a loss of time and money. Loss of data can severely impact the success of a project. An effective server backup and recovery plan is crucial for running a successful server and hosting services.

Table- III: Elements for Employees

Using Personal Social Media
I. Back-Up Procedure
a. Server backups must be performed every night through working days.
b. Backups performed on Friday must be kept for a month before recycling. c. The last backup of every month will be considered as monthly backup and must be kept for a year before recycling.
d. Monthly backup tapes must be stored in a fireproof safe.
e. The last two monthly tapes must be stored off-site in a fireproof safe.
f. Backups that are performed and monitored must be done by a full-time IT employee.
g. Backups will be automated using software products like Veritas Backup Exec, Arc serve or any similar product.
h. Tapes must be inserted routinely every night before leaving work.
i. Backup failures must be reported and action must be taken as quickly as possible.
j. Backups must always be performed before upgrade or any modification to a server.
II. Loss of Data
a. Loss of data is mainly due to a file corruption, virus, security or human error.
b. If loss of data is discovered, investigation team must be immediately dispatched.
c. If due to data corruption, IT staff must troubleshoot and see if the problem is hardware or software related to prevent any addition corruption of files.
d. If due to a virus, IT Staff must determine the core of virus and remove it to prevent further data loss.
e. If due to security, IT Staff must determine the compromise situation and try to fix the vulnerability quickly
f. If due to a human error, IT Staff must be informed by a member and he/she must be trained to avoid any error in future.
g. Restoration of data must be performed after discovery of a core problem.
III. Restoration of Data
a. IT Staff must determine the time and date of the lost data.
b. IT Staff must determine the appropriate backup media to restore the data. c. IT Staff must now insert the backup media into an appropriate server.
d. IT Staff must now run the Backup software, such as Veritas Backup Exec, Arc serve etc.
e. IT Staff must monitor the restoration of data process.
f. IT Staff must contact the end-user of the data to finalize restore.
g. Upon approval from the end-user, the restore process is done successfully.
IV. Disaster Recovery
a. If a disaster is discovered, IT Staff must determine core of the problem and should proceed accordingly.
b. If the disaster is hardware related, IT Staff must handle the failed hardware to the repairable unit and they can see if it can be repaired by applying above mentioned failure methods.
c. If hardware unit is not repairable then it must be replaced and full analysis must be done to prevent similar disaster in future.
d. If disaster occurred naturally such as by rain water, fire, earthquake, etc. then the hardware must be replaced and the server should be restored using the backup media.
e. Upon restoration of data, validity must be checked.
f. IT Staff then contact the end-user of the data to finalize restore as above for successful recovery.

V. CONCLUSION

To conclude this plan and manual, Tech Company must follow this above plan and procedures. They will be successful in setting up a cloud server for Higher Education resources. Each member working in an organisation during set up of servers should go through their roles and responsibilities from this reliability plan for a reliable solution. Engineering based reliability organisation infrastructure is best way to ensure a reliability in an organisation, as it not only assures reliability but also quality because it has a quality manager as well working full time to make sure each component matches to the best quality and he/she is there to throw away any parts or elements which are not up to quality mark.

This way reliability in an organisation will occur and a good way to maintain and manage any activities that will be performed during setting up of a server and for other procedures like setting up a disaster recovery unit and a back-up unit. Tech Company. must also implement ISO/IEC 27000 security standards as mentioned above to keep information assets secure [11]. If all these activities are being handled carefully and through this plan, then surely Higher Education will have a reliable server for Primary and standby operations. On the other hand, security services and recovery services will be ensured and quality based services will increase the durability for Higher Education.

REFERENCES

1. Al-Zyoud M. F. Social Media Marketing Functional Branding Strategy and Intentional Branding. Journal of Problems and Perspectives in Management. 16 (3), 102-116, 2018.
2. Ash J., Anderson B., Gordon R. & Langley P. Digital Interface Design and Power: Friction, Threshold, Transition. SAGE Journal 36(6), 1136-1153, DOI: 10.1177/026377581876426, 2018.
3. Bartin B., Ozbay K., Gao J. & Kurkcu. Calibration and Validation of Larfe-scale traffic simulation networks: a case study. Procedia Computer Science, 130, 844-849, 2018
4. Bauer, E. Design for Reliability. 1st ed. Chicester: Wiley, 2011.
5. Beldick.com. Probability of failure on Demand (POFOD) Calculation, 2017.
6. Dar A. R., & Ravindram R. A Comprehensive Study on Cloud Computing Paradigm. International Journal of Advance Research in Science and Engineering. 7(4), 235-242, 2018.
7. Entsog. Implementation Monitorig and Baseline Effect Monitoring of The Tariff Network Code. Europan Network of Transmission System Operators for gas. Implementation and Effect Monitoring, 2018
8. Fauzi S. S. M., Suali A. J .& Sobri W. A. W. M. A Stateof the Art: Software Configuration Management Tools for Global Software Development. Journal of Physics: Conference Series. DOI: 1088/1742-6596/1049/1/01/2006, 2017.
9. Gokulakrishnan S. Gnanasekar J. M. Efficient and Privacy for Data Integrity and Data Replication in Cloud Computing. International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN : 2278-4075,pp.333-336 Volume-8 Issue-12, October, 2019.
10. Hadzhikoleva S., Hadzhikolev E., Cheresharov S., & Yovkov L. Towards Building Cloud Education Networks. TEM Journal 7(1), 219-224, DOI:10.18421/TEM71-27, 2018.
11. Iso.org. ISO/IEC 27000/270001 Information security management, 2017.
12. Jayaraj T. J., Samath A. Process Optimization of Big Data Centre Using Nature Inspired Firefly Algorithm and K-Means Clustering. International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN : 2278-4075,pp.311-320 Volume-8 Issue-12, October, 2019.
13. Manoj K. A. Mrudula K., Srinivas K. P. Risk Factors and Security Issues in Various Cloud Storage Operations. International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN : 2278-4075,pp.48-52 Volume-8 Issue-12, October, 2019.
14. Mathur M., Madan M. Software Defined Cloud Mini Data Centers-An Effort Towards Reduction in Latency of Cloud Traffic Delivery. International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN : 2278-4075,pp.20-26 Volume-8 Issue-12, October, 2019.
15. Micosoft. Testing for Reliability, Msdn.microsoft.com. 2017
16. Neufelder. Revised IEEE 1633 Recommended Practices for Software Reliability,2017.
17. O'Connor, P. and Kleyner, A. Practical Reliability Engineering, 5th Edition. 1st ed. John Wiley & Sons, 2012.
18. Peroli M., De Meo F., Vigano L & Guardini D. MobSTer: A model-based security testing framework for web applications. Journal of Software Testing, Verification, and Reliability. 28(8), e1685, 2018.
19. Perreault M. C. & Mosconi E. Social Media Engagement: Content Strategy and Metrics Research Opportunities. Proceedings of the 51st Hawaii International Conference on System Science, 2018.
20. Raj C. Jacob A. Performance Evaluation of SUMEGHA Cloud Computing Environment: Methodologies & Tool. Towards Reduction in Latency of Cloud Traffic Delivery. International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN : 2278-4075,pp.875-880 Volume-8 Issue-12, October, 2019.
21. Ramos P. L., Nascimento D. C., Cocolo C., Nicola M. J., Alonso C., Ribeiro L. G.M., Ennes A., & Louzada F. Reliability-Centered Maintenance: Analyzing Failure in Harvest Surgence Machine Using some Generalizations of Weibull Distribution. Journal of Modelling and Simulation in Engineering. DOI: 10.115/2018/1241856, 2018.
22. Sahin C. Social Media Addiction Scale – Student Form: The Reliability and Validity Study. Journal of Educational Technology, 17 (1), 169-182, 2018.
23. Salaki R. J. Analysis and Design of Service Oriented Architecture Based in Public Senior High School Academic Information System. 5th International Conference on Electrical, Electronics and Information Engineering (ICEEIE), 180-186 Publisher IEEE, 2017.
24. Salaki R. J., C. R. Kawet., R Manoppo., & F. Tumimomor. Decision Support System Major Selection Vocational High School in Using Fuzzy Logic Android-Based. International Conference on Electrical Engineering, Informatics, and Its Education, C1-C6, 2015
25. Salaki R. J., Mogea T., & Oroh E. Z. Design Mobile Learning (M-Learning) Android Englihs For Young Learner. International Conference on Electrical Engineering, Informatics, and Its Education, 2015.
26. Salaki R. J & Mogea T. Online Learning as A Paradigm of Learning in Higher Education. 7th International Conference on Psychology, Language and Teaching (ICPLT), 2016.
27. Shimizu H., Otsuka Y. & Noguchi H. Design review based on failure mode to visualise reliability problems in the development stage of mechanical products. International Journal of Vehicle Design, vol. 53, pp. 149- 165, 2010.
28. Sutherland, K., Davis, C., Terton, U., & Visser., I. University Student Social Media Use and Its Influence on Offline Engagement in Higher Educational Communities. Student Success, 9(2), 13-24. DOI: 10.5204/ssj.v9i2.400, 2018.

AUTHORS PROFILE

Salaki Reynaldo Joshua Bachelor of Education in ICT (Softaware Engineering), Universitas Negeri Manado Indonesia, Master of Science in Computing (Information Technology Management), Staffordshire University United Kingdom, and Master of Science in Computing (Information Technology Management), Asia Pacific University of Technology and Innovation Malaysia. Research in last five years, Agile Analytics: Applying in the Development of Data Warehouse for Business Intelligence System in Higher Education, A Comparative Analysis of Extract, Transformation and Loading (ETL) Process, Analysis and Design of Service Oriented Architecture Based in Public Senior High School Academic Information System, Extract Transformation Loading from OLTP to OLAP Data Using Pentaho Data Integration, Online Learning As A Paradigm of Learning in Higher Education, Design Mobile Learning (M-Learning) Android English for Young Learners, Decision Support System Major Selection Vocational High School in Using Fuzzy Logic Android Based.

Tini Mogea Bachelor in Education, English Education, Universitas Negeri Manado Indonesia, Master of Humanities, American Studies, Universitas Gadjah Mada Yogyakarta Indonesia, and Doctor in Education, Education Management, Universitas Negeri Jakarta Indonesia. Lecturer at English Education Department, Universitas Negeri Manado, Indonesia, Reviewer for Ministry for Research, Technology and Higher Education, Research for last 5 five years, The Influence of Calculative Commitment Toward Lecturers Work Productivity at Faculty of Language Arts State University of Manado, Curriculum and Lesson Planning: Outpacing Learning Process through Evaluation on English Textbook in Senior High School, Friendship in White's Charlotte Web, Discrimination InSocial Relation in Faulkner's Light in August, Design Mobile Learning (M-Learning) Android English for Young Learners.