

Privacy and Statement

Statement of Anonymity & Non Competition

WebServer agrees not to divulge ourselves as your source for Web hosting. We value our resellers and will not contact or solicit the Reseller's customers. WebServer may be listed in the DNS registry's Whois database as the Zone Contact and/or as the authoritative name server for the domain. Reseller will be listed as the Administrative, Technical or Billing Contact. However, if the reseller's customer contacts WebServer due to a lack of service or performance by Reseller, we will not refuse the customer support or service. We believe this policy best protects the customer and provides uninterrupted service.

WebServer is committed to first-rate customer service. We provide 24/7 phone support. However, the fastest way to contact our technical support department is via our email at support@webserver.com.my to open an online trouble ticket.

Private Policy

While information is the cornerstone of our ability to provide superior service, our most important asset is our customers' trust. Keeping customer information secure, and using it only as our customers would want us to is a top priority for all of us at WebServer.

We will safeguard, according to strict standards of security and confidentiality, any information our customers share with us.

We will limit the collection and use of customer information to the minimum we require to deliver superior service to our customers, which includes advising our customers about our products, services and other opportunities, and to administer our business.

We will permit only authorized employees, who are trained in the proper handling of customer information, to have access to that information. Employees who violate our Privacy Policy will be subject to our normal disciplinary process.

We will not reveal customer information to any external organization unless we have previously informed the customer in disclosures or agreements, have been authorized by the customer, or are required by law.

We will always maintain control over the confidentiality of our customer information.

Whenever we hire other organizations to provide support services, we will require them to conform to our privacy standards.

For the purposes of credit reporting, verification and risk management, we will exchange information about our customers with reputable reference sources and clearinghouse services.

We will attempt to keep customer files complete, up to date, and accurate. We will tell our customers how and where to conveniently access their account information (except when we're prohibited by law) and how to notify us about errors, which we will promptly correct.

Minimal Data Backup Policy

- **Purpose:**
ACSB shall not be liable for any taxes or other fees to be paid in accordance with or related to purchases made from Client or ACSB's server. Client agrees to take full responsibility for all taxes and fees of any nature associated with such products sold.
- **Applicability:**
Dedicated Server only
- **Background:**
Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. The ongoing availability of data is critical to the operation of the company or individually. In order, to minimize any potential loss or corruption of this data. Responsibility for providing and operating administrative applications needs to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

Threat Scenario:

The following typical threat is assumed for a data backup policy as part of minimal baseline protection:

- Demagnetization of magnetic data media due to ageing or unsuitable environmental conditions (temperature, air moisture)
- Interference of magnetic data media by extraneous magnetic fields
- Inadvertent deletion or overwriting of files
- Technical failure of storage device (head crash)
- Faulty data media
- Uncontrolled changes in stored data (loss of integrity)
- Deliberate deletion of files with computer viruses, etc.

Policy:

Computer systems that create or update mission critical data on a daily basis need to be backed up on a daily basis to minimize the exposure to loss of mission critical data. The unit responsible for providing and operating such systems must conduct a systematic and detailed investigation of all the influencing factors leading to the compilation of a Minimal Data Backup Policy.

Minimal Data Backup Policy:

The minimal data backup policy stipulates the following:

- **Software:**
All software, whether purchased or created personally, is to be protected by at least one full backup.
- **System data:**
System data are to be backed up with at least one generation per month.
- **Application data:**
All application data are to be protected by means of daily full backup.
- **Storage:**
All backups are to be stored in the network access storage server.

Guidelines

- **RETENTION:**
Backup retention will be available for 7 days, the system will automatic overwrite the backup after 7 days.
- **PERSON-IN-CHARGE:**
Each data backup process should have at least one primary person-in-charge and one substitute. Data backup is a critical security measure thus the relevant persons-in-charge should be committed in writing to adherence to the specific data backup (if established) or minimal data back up policies and procedures.
- **TRAINING:**
All persons-in-charge of data backup should receive adequate training on the data backup process, data restoration process, retention and storage. Regular refresher, motivation campaigns and adherence checking on data backup must be conducted.
- **DOCUMENTATION:**
Documentation is necessary for orderly and efficient data backup and restoration. Once the backup is in process, a log file will be sent via e-mail to the person-in-charge, whereby to notify the status of the backup. If, there is an error from the log file, the person-in-charge will check the on backup set. This is to ensure that the person-in-charge is able to monitor the whole process of the backup, where an immediate action could be taken when any problems occurs.
- **RESTORATION OF DATA:**
The restoration of data using data backups must be tested at irregular intervals, at least after every modification to the data backup procedure. It must at least once be proven that complete data restoration is possible (e.g. all data contained in a server must be installed on an alternative server using substitute reading equipment to the data backup writing equipment). This ensures reliable testing as to whether:
 - Data restoration is possible
 - The data backup procedure is practicable
 - There is sufficient documentation of the data backup, thus allowing a substitute to carry out the data restoration if necessary
 - The time required for the data restoration meets the availability requirements

This is a computer generated page. This page not require any signature.

3

- This restoration of data service is provided ONCE a month at no additional charge. Should any further request for additional restore service is required; RM 250 will be charged for each service. Unutilized restore services provided free are not able to carry forward.
- **RECOVERY SOLUTION FROM THE BACKUP SOLUTION:**
There is a need of approximately 4 hours to recover back the system when the system is crash or problem with the hard disk.
- **BACKUP COVER:**
The backups are on the operating system; web application and database with log files of each.
- **BACKUP TYPE:**
The implementation of the backup is on a full backup system instead of incremental backup.
- **FREQUENCY OF BACKUP:**
A weekly basis backup is on for the operating system. In daily basis will be performing to backup the web application and database.
- **SIZE OF BACKUP:**
The size of backup are depends on the plan that been subscribed, the details as following:

Plan	Size of Backup Space
RM 200/month	2 GB
RM 500/month	5 GB
RM 800/month	10 GB
RM 1,200/month	20 GB

- **DURATION OF THE BACKUP:**
It is dependent on the total size of files or folders that required to be backup. As an example, 15GB backup will required an estimated time of 180 minutes.
- **BACKUP PROCEDURE:**
There is a need of the users' login in order the backup process could be done.