

Data security policy

Nyama Catering Ltd is committed to ensuring the security of personal data held by the company. This policy is issued to all staff with access to personal data at the company and will be given to new staff during their induction. If any member of the team has concerns about the security of personal data within the company they should contact Johannes Burger.

All members of the team must comply with this policy.

Confidentiality

- All employment contracts and contracts for services contain a confidentiality clause, which includes a commitment to comply with the company's confidentiality policy
- Access to personal data is on a 'need to know' basis only. Access to information is monitored and breaches of security will be dealt with swiftly by Johannes Burger
- We have procedures in place to ensure that personal data is regularly reviewed, updated and, when no longer required, deleted in a confidential manner. For example, we keep records for at least 10 years.

Physical security measures

- Personal data is only removed from the company's premises in exceptional circumstances and when authorised by Johannes Burger. If personal data is taken from the premises it must never be left unattended in a car or in a public place
- Records are kept in a lockable fireproof cabinet, which is not easily accessible by staff and visitors to the company
- Efforts have been made to secure the company against theft by, for example, CCTV, lockable doors



- The company has in place a business continuity plan in case of a disaster. This includes procedures for protecting and restoring personal data.

Information held on computer

- Appropriate software controls are used to protect computerised records, for example the use of passwords and encryption. Passwords are only known to those who require access to the information, are changed on a regular basis and are not written down or kept near or on the computer for others to see
- Daily and weekly back-ups of computerised data are taken and stored in a cloud based system
- Staff using practice computers undertake computer training to avoid unintentional deletion or corruption of information
- Precautions are taken to avoid loss of data through the introduction of computer viruses.
- Data stored on cloud computing facilities has in place a rigorous service level agreement with our cloud provider to ensure that all our obligations in this policy are fulfilled and that all information is secure.