LetMC.com®

Security Features: *Lettings & Property Management Software*

V 2.0 (23/02/2015)

Table of Contents

Introduction to Web Application Security

The Lettings & Property Management software constructed by LetMC follows an industry standard software development lifecycle and is constantly evolving to meet the demands of our clients. New versions of the software, which include additional functionality and defect fixes, are developed and tested by our highly experienced IT team before being released, typically in 6-8 week cycles, to our clients.

Our web based software is built by certified software developers using robust .Net framework and the latest version of SQL.

All the computers in our offices are protected by advanced firewalls and further covered by McAfee Enterprise security software, ensuring that they are clear of any viruses and unauthorised access by hackers is prevented.

Client data is automatically backed up every fifteen minutes to Amazon's virtual servers, no data is kept on site. In the highly unlikely event of a critical system failure, our clients' data is still safe.

LetMC is continuously striving to ensure that our letting management software is scalable to meet the demands of both start up companies and also established multi-branch agents. However, regardless of the size of the company, LetMC's software architecture and infrastructure provides a robust and meticulous approach to security.

Potential Security Vulnerabilities for Web Applications

Web based applications are particularly vulnerable to attacks from external as well as internal sources. The three main threats to system architecture are:

- Software vulnerabilities that may allow hackers to gain access to system
- Hardware vulnerabilities (in the supporting server systems)
- Weaknesses in client websites that may allow access via a back-door

LetMC remains vigilant against these threats and the measures currently being undertaken to counteract them are detailed in the following points.

LetMC System Architecture

Network Security: Penetration and Vulnerability Testing

In order to test the robustness of LetMC's online applications, an independent team of network and system testers have subjected the Lettings & Property Management software and hardware to rigorous black box penetration testing. The overall results of the independent penetration testing found the software to be robust.

All pages on the Lettings & Property Management software are protected by SSL. All web pages are held securely on our web servers and in source control. SSL certificates are used to encrypt web traffic should the client decide to use our HTTPS service. SSL certificates are used to ensure that web traffic over HTTPS is provably correct at the client-side, i.e. is the same information as that sent.

Furthermore, the system can be locked down to a range of IP addresses. This allows users to control where it is possible to gain access to the system. Whether it is locking down the entire system to the confides of the office's network or blocking a certain IP address range to prevent users from gaining access in that location.

Software Security Functionality

The software includes a number of features which increase the overall security of the Lettings & Property Management software:

1. System requires “strong” passwords. Passwords. More details on request.

2. Security Options on a per company basis:
   1.1 Username to be optionally displayed. The username displayed at the top of the LetMC system can be switched off through Control Panel>Security Config>Interface Preferences. Some companies may deem the displaying of the username as a security risk.
   1.2 Forced password change and remebering previously stored passwords. More detials on request.
3. Anti-hacking Security Measures:
   3.1. When a staff member is in the process of logging into LetMC, if an incorrect username or password is entered, the system clears the ‘Password’ box and a pop-up message informs the user that an ‘Invalid username or password’ has been entered.
   3.2. If a staff member enters their correct username and an incorrect password X times (more details on request) in succession, while attempting to log into their account on LetMC, then their account will be locked-out. To unlock the account a higher level user must re-activate the staff member and re-set their password.

4. Security Audit Report. An audit entry is made each time:
   a. staff member’s password is changed
   b. new staff member is added including their user level
   c. staff member's log-in has been locked because of too many failed log-in attempts
   d. new landlord, tenant or contractor is added including their bank details
   e. landlord, tenant or contractor’s bank details are changed.
   f. Enabling/Disabling the Paid Sales functionality
   g. Adding a new IP Filter entry
   h. Staff Access level change
   i. Too many login attempts
   j. Name of staff member who generated the RSTB, People in Credit/Debit reports.

5. Restrictions have been put in place to prevent staff members from logging into the system from more than one machine. If the user is logged in on say the office computer and then logs in on a different computer, the system will automatically log them out of the office computer.

6. Secure Web Pages via SSL. All pages within the Lettings & Property Management web application is transmitted over https:\\ which displays a small padlock at the bottom of your screen.

7. IP Lock Down. As previously mentioned, there is a section within the system that allows users to enter an IP address to either allow or disable access to the system from that location.

Staff Activity Restrictions

Restrictions are in place throughout the LetMC software to regulate that only staff with high level of security clearance are able to access and update critical company information, thus ensuring a high level of defence against staff errors and information leakage (which can result if transient members of staff are compromised). Customisable staff activity restrictions, which apply regardless of whether a user level is able to access a node, include:

- Changing Bank Details - protects the tenant, landlord, contractor and company from having their bank account name, account number or sort code changed.
- Contra Transaction – restricts the user level that can perform a contra on a transaction while not affecting the level of user able to view accounts and transactions.
- Change Signed Rent Schedule – restricts the level of user that can make changes to the payment or rent schedule for a signed tenancy while not affecting the level of user able to Modify Instruction / Tenancy.
- Change Utility Responsibility – For a signed tenancy this protects the recording of whether landlord or tenant is responsible for water, electricity, gas or council tax. Update new audit
- End Signed Tenancy – Controls what user level is allowed to set the end date of an active tenancy.

Hardware Perspective: Server Backup and Security

All LetMC's client data is held in S3 buckets in our Amazon account. Access to this account is limited to specific staff members in our IT department. Amazon applications and their data are protected by highly secure facilities and infrastructure, but they're also protected by extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection and password brute-force detection on AWS Accounts.

Users are then able to implement their own security processes on top of Amazon's to further protect their systems and data.

More information can be found here: http://aws.amazon.com/security/ and also in the Amazon Web Services: Overview of Security Processes document.

Our web based lettings software automatically backs up customer data every 15 minutes to our AWS account. The AWS platform provides a solid and reliable infrastructure to ensure our customer's data is always at their fingertips.

Advanced firewalls, further protected by McAfee Enterprise security software, ensure that any viruses and hackers are kept out of our staff computers, as well as our local file server.

Node Access Security Customisation

LetMC can specify staff user level access restrictions on a per company basis. Each node in the system can be individually restricted to a minimum user access level independently for each company, thus allowing the system to be tailored to meet the needs of each client. Five user access levels are available: Client Colleague, Client Staff, Client Manager, Client Finance, Client Administrator and each node has a 'default' user access level which applies when a company is first set up and remains in place until the access level is changed. User levels that have been restricted from accessing the nodes are not able to view or edit the nodes.

1. Node Access Levels. The node access security restrictions can be tailored to meet the needs of individual companies and help to ensure that the system is scalable and flexible for both small single branch companies and also for large multi-branch companies.

    1.1 All nodes can be customised to restrict user access levels including Accounting and Reporting nodes.
    1.2 Certain nodes which contain critical company contact information, such as Mail Merge> Active Landlords list, are programmed to not be display for user levels below Client Manager, even when the node's access level has been reduced below this user level.

2. Multi-Branch Staff Restrictions. Staff members can be restricted to only view their own Branch Information (i.e. the Branch Selector cannot be used). Multi-Branch Staff Restrictions work in conjunction with the Multi-County restrictions and group the views together into the same related areas. Restricted staff cannot view reports for other branches in their company.

3. Multi-Branch Finance Reporting - the staff member is restricted to only viewing their own Branch information on the following accounting reports:

    - Invoiced Sales Income
    - Un-invoiced Sales Income
    - Tenant Bond Deposits Held
    - Debtors and Creditors

4. Multi-County Staff Restrictions. Staff members can be restricted to only view branches within their own 'county' by setting the Multi-County Staff Restrictions selectors. The Multi-County Staff restrictions group the nodes together into related areas such as General Views, Applicant Views, Reporting (all non-finance reporting), and Finance Reporting (finance reports). The Multi-County and also the Multi-Branch Staff Restrictions are particularly useful for companies that have franchise branches that must not have access to another branch's financial or reporting data.

Technical Information

System Security

Security classification scheme:

- Software: there is a system administration login level which allows LetMC staff users to view client data. LetMC privacy policy states that customers of the service will be using the site to host data and information ("Data"). LetMC will not review, share, distribute, print, or reference any such data except as provided in the Letmc.com Master Subscription Agreement, or as may be required by law.

- Individual records may at times be viewed or accessed only for the purpose of resolving a problem, support issue, or suspected violation of the Master Subscription Agreement, or as may be required by law. Of course, customers are responsible for maintaining the confidentiality and security of their user registration and password. All subsequent levels are client controlled; they are 'Client Administrator', 'Client Finance', 'Client Manager', 'Client Staff' and 'Client Colleague'. Hardware: Physical access to hardware that stores data is restricted to the IT team, who are under the direct management of Ieuan Williams, Head of IT and System Network Administrator, and a Company Director.

Availability of Business Information

LetMC regularly reassesses the impact of business information being unavailable:

- Letmc.com service is an online subscription service. Full Terms & Conditions are published on our website. The target key performance indicator is an uptime of 99.80% (between 6am and 10pm, excluding planned downtime on Mondays from 7pm onwards).

Robust and Reliable Computer Systems

Our Amazon virtual machines run on Microsoft Windows Server 2010 and make use of the latest version of SQL. Updates are carried out regularly on these machines.

Measures to Physically Protect Critical Facilities

LetMC:

- All staff machines are locked down with cab lock components and are password protected.
- Each member of our IT team has UPS (Uninterrupted Power Supply) units that provide continual power, for up to 30 minutes, in the event of outage. This means that they are still able to upload changes/fixes to our Amazon account if something was to happen to that whilst we suffered a power cut.
- Our local file server, that contains client information and other sensitive documents, is protected by our Sonic Wall firewall and is also locked in a server cabinet. Specific user levels have been created for all staff members who need access to it. This prevents them from seeing documents that they shouldn't.

Amazon:

- AWS's data centres are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centres. This experience has been applied to the AWS platform and infrastructure. AWS data centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
- AWS only provides data centre access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centres by AWS employees is logged and audited routinely.

This information was taken from Amazon Web Services: Overview of Security Processes document.

Event Logging

All server systems have logging enabled (i.e. Windows event logs), and our application software also has full auditing capabilities. Our Network and System Administrators perform these tasks regularly, and system event logs are monitored daily.

System/Network Logging

An alert system has been put in place to notify our System and Network Administrator of firewall logs with all untoward traffic highlighted, as well customised AWS notifications that report on certain performance/usuage statistics and errors that occur with the system.

Firewall routing for network traffic

LetMC use a SonicWall to prevent unauthorised access. Only the Network Administrator is allowed access to its configuration controls, and all change requests must be passed through to this person for evaluation and potential configuration.

Appendix

Appendix I

FAQ's

Q. Do LetMC have disaster recovery contingency plans?
A. All of the LetMC system's data is located in one of Amazon's availability zones. If for some reason this zone was to fail then our system would automatically switchover to one of the other availability zones.

In the unlikely event of a total failure of the primary availability zone, we aim to have the LetMC system restored and up and running within 1 hour of the failure with restricted service. The data used will be a snapshot of the system no older than 30 minutes before the critical failure time.

Q. Do LetMC use data encryption (SSL etc.)?
A. All pages of the Lettings & Property Management web application are encrypted using SSL.

Q. Is there a maintenance schedule for updates?
A. We have a scheduled maintenance window every Monday at 7pm. Updates are deployed within this window, but not every Monday night, the cycles are typically scheduled every 6-8 weeks.

Q. What back up procedures are in place?
A. Data is automatically backed up to Amazon's S3 service every 10 minutes. There is also an option in the system to generate an XML critical backup file. This file contains data such as:

- Details and balances of all accounts in the system
- All landlord, tenant, contractor and property details
- Tenancy information and corresponding maintenance jobs, inventory detials etc

It can be manually downloaded by a staff member, or it can be included in one of our overnight FTP feeds. The file is protected by a randomly generated password.