2022

MSL System™ Elections security overview

Membership Solutions Ltd
Warwick SUHQ
University of Warwick
Gibbet Hill Rd
Coventry
CV4 7AL
United Kingdom

Tel: +44 (0) 330 828 1837
info@ukmsl.com
www.ukmsl.com
UK Company reg 5525449

The MSL System™ helps students' unions, associations, guilds, universities, and colleges of all sizes provide more engaging, accessible, and effective services for students at every point of their journey through education.

At MSL, we are dedicated to helping student organisations optimize the running of their elections. Our innovative approach enables us to deliver election systems and products that are secure, auditable, flexible, and transparent.

More information about MSL and the MSL System is found on our website https://www.ukmsl.com

How your data is used to ensure the integrity of the election

For our customers to gain maximum benefit from the MSL System, we request regular access to an up-to-date set of data for all individuals who have opted to share their data with the respective institution.

The University, or other institution, provides a data file containing student data to pre-register users onto the System. This allows them to be verified as bona fide current students to enable website access, voting, purchasing, participation in activities and the receiving of electronic messages. If a data file is not provided, then data attributes are released via the Single Sign On login, or data provided by the user via a registration page, usually with an email regex to verify student status.

If a data file is supplied, a secure upload location is created in an Amazon data region specific to the customer's jurisdiction, where the S3 bucket is subject to Amazon server-side encryption ready to be transferred to the MSL servers. Once the data reaches the MSL servers it is stored in a secure location on disk while it waits to be imported. Once imported, the file is deleted. Now secure in the MSL System database, data is only accessible to MSL system administrators and authorised admins at the customer's organisation.

This data can be used to carry out and make automated decisions on behalf of the customer where such decisions are based on criteria set by the customer (for example, where a decision is made on whether a student may vote in an election based on their eligibility under the customer's elections regulations).

Checking election eligibility

Once the student logs into the customer's website, the system checks they meet both the election's visibility settings and the requirements set against each post added to the election. This verifies that the student can participate as a candidate and/or voter before allowing them to nominate themselves or cast a vote against one or more posts.

To prevent more than one vote from being cast per post by a user, the system has certain safeguards in place to prevent duplicate accounts from being created for the same person, for example, if a student record appears twice in the data file, or the student has created a guest account on the website before they appear in the data import. A data record is added to the

pending import table ready for the accounts to be merged if it cannot be imported automatically due to another account appearing in the customer's MSL System with similar details. A data record is added to the import duplicates table if duplicate records are found in the latest data file e.g. two records in the data file for the same student. The primary record will be selected and added to the system, and the secondary, or incorrect record is added to the block list, preventing the student from being able to log into the website on two separate accounts.

Votes cast are linked to the voter's account in the MSL System. Depending on the options provided by the customer, the voter can cast their vote on the website, polling station or StudentLink app. If there is more than one post within the election, the voter can vote for the different posts on a combination of all devices, however, only one vote can be cast per post unless vote changes have been enabled.

The elections profile page at /elections/profile/ displays the elections and positions the voter has voted for, alongside the date and time the vote was cast. Election notifications can be configured by election admins to notify voters when votes are cast against their accounts. The vote acknowledgement notification is sent to voters each time they cast a vote, and the voting completion notification is sent to voters when they have voted for all the posts for which they are eligible.

Voter privacy

No outside observer, including MSL staff and elections administrators, can determine for whom a voter voted if the vote/voter link is disabled in the MSL System setup. If the vote/voter link is enabled, no outside observer, including MSL staff and elections admins, can determine for whom a voter voted unless, in cases where candidates or voters are being investigated for coercing their fellow members into voting a certain way, for example, a vote export is created accessible only to MSL staff and authorised elections admins.

MSL System™ security

The MSL System is hosted in the cloud by professional third-party datacentres, and therefore physical and electronic access is very tightly controlled. We ensure all traffic (including that containing personal data) to and from the MSL System is encrypted under HTTPS and ensure the MSL System is subject to regular vulnerability scans by a third-party security system and the results acted upon by MSL technical staff.

The MSL development framework and operational environment features built-in safeguards against risks including many of those in the OWASP Top 10. Secure standards are applied in the development of the MSL System.

MSL operates an Information Security Management System (ISMS) aligned to ISO 27001: 2013 and PCI (Payment Card Industry) DSS v3.2 and is reviewed at least annually. MSL ensures persons authorised to handle personal data are trained and fully aware of their obligations in maintaining the confidentiality of personal data. MSL staff are subject to a confidentiality agreement as part of their contract of employment. In addition, mandatory annual data protection and information security training is undertaken by all staff which requires a pass certificate to be submitted to confirm compliance.

MSL restricts access to customers' personal data only to permanent MSL staff and then only to those who need it to deliver the System and the Services through rigorous management of internal systems access. We control direct access to MSL System databases, permitted only by permanent MSL staff with relevant permissions and then only allowed from IP addresses fixed to the MSL office. No outside access is permitted.

Data Centre security

United Kingdom, Ireland, and the United Arab Emirates

Data security is paramount at ANS. Their ISO 27001-certified and PCI-compliant data centres have the highest level of protection from both virtual and physical security threats. They also have a team of security specialists whose job is to ensure our customers' data is secure in the ever-evolving cyber-security landscape.

Australia and New Zealand

Amazon Web Services (AWS) is architected to be the most flexible and secure cloud computing environment available today. Their core infrastructure is built to satisfy the security requirements for the military, global banks, and other high-sensitivity organisations. This is backed by a deep set of cloud security tools, with over 300 security, compliance, and governance services and features. AWS supports 98 security standards and compliance certifications, and all 117 AWS services that store customer data offer the ability to encrypt that data. AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014.

Canada

Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the Microsoft Azure datacentre resources. Data centres managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data centre floor. The Azure infrastructure is designed and managed to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.