

# ATGS Data and System Security Protection Guide



At Ally Techno Grit Solutions Corp., keeping your personal information safe is our top priority. Our systems are built on modern, secure foundations to ensure your data remains private, safe, and accessible only to the right people. We understand that technology and security can sometimes sound complicated, so we have created this simple guide to explain exactly how we protect your system and data.

## 1. Where Your Information is Stored

Our platform is built on a reliable, modern foundation. To make sure your data is always accessible and secure, we partner with industry-leading technology providers:

- **Web Address Security:** Our website domain is safely managed through a globally recognized, trusted provider. This ensures your connection to our platform is always safe and authentic.
- **Secure Cloud Storage:** Your information is stored in a highly secure, enterprise-grade cloud database. This guarantees that your personal records are constantly protected by strict, top-tier physical and digital security measures.

## 2. How We Protect Your Data Every Day

We have several automatic safety measures in place to keep your information completely safe from outside threats:

- **Bank-Level Secure Connections:** Whenever you use our website, your connection is locked and encrypted. We use industry-standard secure connections, meaning any information you type into our website is scrambled so that no one else can read it.
- **Strict Password Protection:** We never store your actual password in a readable format. Instead, we use a complex mathematical process to completely scramble it. This means even our own staff cannot see your password.
- **Automatic Logout:** If you step away from your computer and forget to log out, our system will automatically log you out after a period of inactivity. This ensures no one else can sit at your screen and view your account.
- **Safe Information Handling:** Our system is programmed to strictly double-check all information before accepting it. This ensures that malicious software cannot be sneaked into our database.

- **Hidden Personal Details:** Your sensitive information is never exposed in the system's background code or web address bars.
- **24/7 Monitoring and Defense:** We have an active digital alarm system and firewalls that constantly watch for any suspicious activity. This system records system movements, immediately blocks unauthorized access, and logs tracking information.

### 3. Who Can Access Your Data (Access Controls)

- **Strict Account Verification:** User accounts are not created automatically. They are carefully set up and validated by our Administrators to ensure only authorized users have access.
- **Secure Digital Badges:** When you log in, the system assigns you a highly secure, temporary "digital badge". This badge expires automatically if you are inactive. Additionally, logging into a new device will safely log you out of your old one.
- **No Auto-Fill Risks:** To prevent someone else from sitting at your computer and logging in, our system actively blocks web browsers from automatically filling in your sensitive login information.
- **Customized Access Limits:** Administrators can set up specific access roles for each user. This allows them to strictly control which specific modules and information each user can see. This capability can also be used to hide specific parts of the system or make them read-only based on the user's job requirements.

### 4. Daily Backups and Disaster Recovery

We know how important your records are, which is why we follow strict professional practices to ensure your data is never lost:

- **Daily Data Backups:** Our technical team performs automatic, daily backups of all system data. In the unlikely event of an emergency, server issue, or technical glitch, your information is completely safe and can be quickly restored.
- **Reliable Cloud Infrastructure:** Our database is housed in a premier, enterprise-grade server environment. This environment is designed with strict physical and digital safeguards to protect against hardware failures and natural disasters.

### 5. Continuous Monitoring and Safe Operations

- **Activity Logs:** We maintain a secure log of all system activity. If suspicious behavior occurs, our security tools catch and block it immediately.

- **Strict UAT Testing Before Updates:** Before any new features are added to the system, they undergo thorough testing to ensure they meet our high safety standards and fit user requirements. We also keep our "testing" areas completely separated from the live system you use.

## 6. Your Rights to Your Information

This is your personal information, and you always have control over it. You can freely request a copy of your personal data at any time, and our team will happily and promptly provide it to you.

## Appendix: Technical Security Specifications

*The following table outlines the specific technical configurations and protocols applied to our MAS application system architecture.*

| Security Category                    | Implemented Measure / Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network &amp; Transport</b>       | <ul style="list-style-type: none"> <li>• System is defaulted to HTTPS; HTTP access will not retrieve content.</li> <li>• Applies SSL and uses TLS 1.2 and 1.3.</li> <li>• Let's Encrypt applied for the server and client program code certificates.</li> <li>• Redirect destinations are limited by registered IDs defined by system routes.</li> <li>• External transitions use HTTP 302 responses and explicit Location headers.</li> <li>• Connection destinations for client programs are limited to linked web applications.</li> </ul> |
| <b>Authentication &amp; Accounts</b> | <ul style="list-style-type: none"> <li>• Passwords are not stored in plain text; stored as bcrypt hash values.</li> <li>• User accounts setup by Admin based on validated user data and emails.</li> <li>• System prompts if an existing account is being setup.</li> </ul>                                                                                                                                                                                                                                                                   |

| Security Category                                 | Implemented Measure / Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | <ul style="list-style-type: none"> <li>• Confirmation URLs for new accounts are one-time use with a set expiration date/time.</li> <li>• Re-logging into a new terminal/device logs out the previous session.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p align="center"><b>Session Management</b></p>   | <ul style="list-style-type: none"> <li>• Session IDs generated via Laravel Frameworks using secure, 32-byte random strings.</li> <li>• Laravel defaults applied (strong encryption, session hijacking prevention).</li> <li>• Current time (milliseconds) used as seed for random number initialization on startup.</li> <li>• System has session control and expiry; Apache applies limits to session ID validity time.</li> <li>• Explicit logout function provided.</li> <li>• New session ID issued upon completed authentication; maximum issue values are set.</li> <li>• Session IDs sent as cache backend, not embedded in URLs.</li> <li>• Hidden parameters/URLs do not contain user IDs; identity is checked via session ID.</li> <li>• Input errors do not update the session; session is retained.</li> <li>• Important objects are signed, checked for integrity, and not serialized in hidden parameters or saved as local files.</li> </ul> |
| <p align="center"><b>Application Security</b></p> | <ul style="list-style-type: none"> <li>• WAF captures attack-related network logs; OS captures security-related logs.</li> <li>• Audit Trail/System History logs all system movement.</li> <li>• Responses do not contain entered user IDs/passwords or unnecessary platform error info.</li> <li>• System defaults to POST method; avoids GET for requests/processes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Security Category                    | Implemented Measure / Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      | <ul style="list-style-type: none"> <li>• Auto-fill/Auto-complete is disabled.</li> <li>• Ajax and Javascript kept to a minimum and only accessible on select code parts.</li> <li>• Input data validity checked (format, length, positive/negative values, context).</li> <li>• Special symbols and line-break codes in input data are escaped for HTML output.</li> <li>• SQL statements escape special symbols; wildcards not used in URL mapping.</li> <li>• External APIs utilize specific security measure lists; server does not call external commands.</li> <li>• Image/video uploads checked for matching MIME types and safe file sizes.</li> </ul> |
| <b>Data Protection &amp; Privacy</b> | <ul style="list-style-type: none"> <li>• Cookies set with Secure and HttpOnly attributes; scripts cannot access cookies.</li> <li>• Username displayed on topnav; Address/Status bars always visible (no frames applied).</li> <li>• robots.txt configured so URLs with valid session IDs are not indexed by crawlers.</li> <li>• META tags and HTTP headers prevent browser caching of sensitive server info.</li> </ul>                                                                                                                                                                                                                                     |
| <b>Development &amp; Deployment</b>  | <ul style="list-style-type: none"> <li>• Continuous monitoring of software version upgrades for security hole fixes.</li> <li>• Web application assessments performed during development and verified with vendors.</li> <li>• Security measure level evaluated as D (Low risk, no action required).</li> </ul>                                                                                                                                                                                                                                                                                                                                               |

| Security Category | Implemented Measure / Protocol                                                                                                                                                                                                                                                            |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <ul style="list-style-type: none"><li>• File paths strictly use relative paths; specifying upper paths and URL file loading disabled.</li><li>• Strict release procedures: source codes, backups, test programs, and debug options are removed from the production environment.</li></ul> |