**ESY SUNHOME Cybersecurity Description**

In an increasingly interconnected digital landscape, safeguarding sensitive information and ensuring the integrity of digital assets has become paramount. Our comprehensive cybersecurity strategy employs advanced measures to protect against evolving threats and vulnerabilities.

1. **Password Protection:**

Robust password protection is a fundamental aspect of our cybersecurity framework.

* 1. **Password Requirements**

All registered user accounts must have strong passwords, including a combination of letters, numbers, and special characters to minimize the risk of unauthorized access.

* 1. **Password Verification**

After five incorrect password attempts, login attempts are restricted for half an hour. We added an extra layer of security to critical systems and data repositories.

1. **Encryption Methods:**

Data encryption is a cornerstone of our cybersecurity approach.

* 1. **Communication Encryption**

All sensitive data transmitted over the network uses HTTPS encryption technology to ensure confidentiality during transmission.

* 1. **Storage Encryption**

Sensitive data stored on devices is encrypted using the bcrypt encryption method to prevent unauthorized access.

1. **Database Security**

Our cybersecurity measures also concern our database security to maintain the integrity of our digital infrastructure.

* 1. **Cloud Database Security**

Utilizing Amazon Cloud Database with Web Application Firewall (WAF), master-slave configuration, and geographically dispersed disaster recovery method to ensure data security and prevent data loss.

1. **User Education and Awareness:**

Recognizing the human element as a critical factor in cybersecurity, we prioritize user education and awareness programs.

* 1. **Security Training**

Providing training session to all users to help them understand the importance of strong password practices, the risks of phishing attacks, and the significance of adhering to cybersecurity policies.

* 1. **Security Awareness**

Enhancing user awareness of network threats and security protection, encouraging the report of any suspicious activities.