INFORMATION SECURITY POLICY

Xtream Markets Ltd

Registration Number: 84516

Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands – MH96960

Website: www.xtrememarkets.com

Email: support@xtrememarkets.com

Effective Date: September 2015

---

1. INTRODUCTION

Xtream Markets Ltd ("Company") recognizes the importance of protecting information assets, client data, trading systems and technology infrastructure.

This Information Security Policy establishes the framework used to protect the confidentiality, integrity and availability of information.

The objective of this Policy is to maintain secure operations while protecting Clients, employees and business systems from security threats.

---

2. POLICY OBJECTIVES

The Company aims to:

- Protect client information;
- Protect trading systems;
- Prevent unauthorized access;
- Maintain data integrity;
- Ensure business continuity;
- Detect and respond to security incidents;
- Reduce cyber security risks.

---

3. SCOPE

This Policy applies to:

- Employees;

- Contractors;
- Consultants;
- Service Providers;
- Third-Party Vendors;
- Technology Systems;
- Trading Platforms;
- Websites;
- Databases;
- Communication Systems.

---

4. INFORMATION ASSETS

Information assets include but are not limited to:

- Client Information;
- Account Records;
- Trading Data;
- Financial Records;
- Compliance Documentation;
- Email Communications;
- Internal Business Information;
- Technology Infrastructure.

All information assets must be appropriately protected.

---

5. INFORMATION CLASSIFICATION

Information may be classified as:

Public Information

Information approved for public distribution.

Internal Information

Information intended for internal business use.

Confidential Information

Information requiring restricted access.

Restricted Information

Highly sensitive information requiring enhanced protection.

Access shall be granted according to business requirements.

---

6. ACCESS CONTROL

Access to systems and information shall be limited to authorized individuals.

Access rights shall be granted according to:

- Job responsibilities;
- Operational requirements;
- Security principles.

The Company applies the principle of least privilege whenever possible.

---

7. USER AUTHENTICATION

The Company may implement:

- Password Protection;
- Multi-Factor Authentication (MFA);
- Security Monitoring;
- Session Controls.

Users are responsible for maintaining confidentiality of access credentials.

---

8. PASSWORD REQUIREMENTS

Users should:

- Use strong passwords;
- Avoid password sharing;
- Change passwords where compromise is suspected.

The Company reserves the right to enforce password policies where necessary.

---

9. CLIENT ACCOUNT SECURITY

Clients are responsible for:

- Protecting login credentials;
- Maintaining device security;
- Monitoring account activity;
- Reporting unauthorized access immediately.

The Company shall not be responsible for losses arising from compromised client devices.

---

10. NETWORK SECURITY

The Company employs security measures designed to protect networks from unauthorized access.

Measures may include:

- Firewalls;
- Traffic Monitoring;
- Access Restrictions;
- Security Controls.

Network protections are reviewed periodically.

---

11. DATA ENCRYPTION

The Company may utilize encryption technologies to protect:

- Client Data;
- Communications;
- Sensitive Information;
- System Access.

Encryption methods may be updated from time to time.

---

12. DATA STORAGE

Information shall be stored using appropriate security controls.

The Company aims to:

- Prevent unauthorized access;
- Protect against data loss;
- Ensure information integrity.

---

13. THIRD-PARTY SERVICE PROVIDERS

The Company may utilize third-party providers for:

- Hosting Services;
- Cloud Infrastructure;
- Payment Processing;
- Trading Technology;
- Data Storage.

Third-party providers may be subject to security assessments where appropriate.

---

14. SECURITY MONITORING

The Company may monitor systems to:

- Detect threats;
- Identify suspicious activity;
- Prevent unauthorized access;
- Maintain operational integrity.

Monitoring may occur continuously.

---

15. CYBER SECURITY RISKS

Cyber security threats may include:

- Malware;
- Ransomware;
- Phishing;
- Social Engineering;
- Unauthorized Access Attempts;
- Distributed Denial of Service (DDoS) Attacks.

The Company maintains measures designed to reduce such risks.

---

16. INCIDENT MANAGEMENT

The Company maintains procedures for responding to security incidents.

Incident response activities may include:

- Investigation;
- Containment;
- Recovery;
- Reporting;
- Remediation.

Security incidents shall be addressed according to their severity.

---

17. BUSINESS CONTINUITY

The Company maintains business continuity measures designed to support continued operations during disruptions.

Such measures may include:

- Backup Systems;
- Disaster Recovery Processes;
- Operational Contingency Plans.

Business continuity procedures may be tested periodically.

---

18. BACKUP PROCEDURES

The Company may maintain backups of:

- Client Data;
- Trading Information;
- Operational Records;
- Business Systems.

Backup schedules and retention periods may vary according to operational requirements.

---

19. EMPLOYEE RESPONSIBILITIES

Employees are responsible for:

- Protecting confidential information;
- Following security procedures;
- Reporting security incidents;
- Maintaining secure working practices.

Failure to comply may result in disciplinary action.

---

20. CLIENT RESPONSIBILITIES

Clients should:

- Use secure devices;
- Maintain updated software;
- Protect passwords;
- Avoid sharing credentials;
- Monitor account activity.

Security remains a shared responsibility.

---

21. SECURITY BREACHES

Where security incidents occur, the Company may:

- Investigate the incident;
- Restrict affected systems;
- Notify relevant parties where appropriate;
- Implement corrective actions.

The Company shall determine the appropriate response based upon circumstances.

---

22. DATA RETENTION

Information may be retained for:

- Operational purposes;
- Compliance requirements;
- Legal obligations;
- Fraud prevention.

Retention periods may vary according to information type.

---

23. POLICY REVIEW

This Policy shall be reviewed periodically.

The Company reserves the right to amend this Policy at any time.

Updated versions shall become effective upon publication on the Company's website.

---

24. CONTACT DETAILS

Xtream Markets Ltd

Registration Number: 84516

Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands – MH96960

Website: www.xtrememarkets.com

Email: support@xtrememarkets.com

Telephone: +357 96 673007

---

25. CLIENT ACKNOWLEDGEMENT

By using the Company's services, the Client acknowledges that:

- They have read this Information Security Policy;
- They understand their security responsibilities;
- They agree to comply with security requirements applicable to their use of Company services.

END OF INFORMATION SECURITY POLICY

Version 1.0