Your fastest way to learn. Why wait?

FIREBRAND

Cyber Security Threat, Statement & Process

June 2017

STATEMENT IN RELATION TO CYBER SECURITY THREAT PROCESSES

Firebrand Training Ltd takes all necessary steps to minimise and remove the risk of cyber security threats relating to the organisation and its customer data.
It is compliant with the Cyber Essentials Scheme, as per most recent assessment in January 2017 and is committed to annual review of its certificate in this regard.
The Head of IT, Bevan Miller, is responsible for all elements of this process, including resolution, though the company works with many experts in the field to ensure best practice.
Our policies and procedures in this regard include but are not limited to the following measures:

THREAT MANAGEMENT

Any identified threat will be reported immediately to the Head of IT, and the board of Directors. The Head of IT will work to assess risks, investigate the threat, identify source, and take remedial action as soon as practical. In line with Data Protection Act requirements, any data breach will be reported to relevant parties as appropriate. The company's insurers will be notified, and Business Continuity Plan invoked if necessary depending on the impact of the threat.

THREAT PREVENTION & MONITORING

Firebrand uses reporting tools within several systems, including with it's Microsoft Azure Estate, and Sophos anti-virus console to monitor potential security threats. Security patching is carried out on a monthly basis to ensure all servers and desktop machines have latest available protections.
Firebrand also engages third party partners to produce a tailored, high-level executive report and an in-depth technical review annually. This report through well-known measures and industry recognised penetration testing methods emphasises high-risk security vulnerabilities and portrays areas for exploitation where applicable. In addition, they provide prioritised remediation efforts.
Latest Penetration Test was carried out:
Date: February 2017
By: Net Consulting Limited. (http://www.netconsulting.co.uk/)

Firebrand operate cyclic testing between penetration vendors to ensure a range of technical process and skills are optimised using different consultancies.

DATA SECURITY

Our Information Assurance capabilities support both our internal requirements for appropriate security controls and those of our customers.
Internal and externally hosted systems are configured and secured by physical, software and process driven security measures. Hot and cold data is stored and with encryption at rest via Microsoft BITLOCKER technologies and encryption hashes in backup vaults.

ENCRYPTION OF DATA AT REST

Email data at rest is encrypted using BitLocker Drive Encryption. BitLocker encrypts the hard drives on a computer to provide enhanced protection against data theft or exposure on computers and removable drives that are lost or stolen, as well as more secure data deletion when BitLocker-protected computers are decommissioned or recycled.

INFORMATION RIGHTS MANAGEMENT

Firebrand has configured Information Rights Management (IRM) to allow the organisation to prevent information leakage by restricting the rights that email recipients have on messages and attachments—such as whether they may forward a message to other recipients, print a message or attachment, or copy and paste message or attachment content.

SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)

S/MIME protects sensitive information by sending signed and encrypted email within Firebrand. Administrators can use remote Windows PowerShell to set up S/MIME after establishing and issuing PKI certificates to users. These certificates must be synchronized from an on-premises Active Directory Certificate Service.
***S/MIME is supported on Internet Explorer 9 or later. Currently, S/MIME is unsupported on Firefox, Opera, and Chrome. For more information, see S/MIME for Message Signing and Encryption.*

IN-PLACE HOLD AND LITIGATION HOLD

When a reasonable expectation of litigation exists, Firebrand can preserve electronically stored information (ESI), including email that's relevant to the case. This expectation can occur before the specifics of the case are known, and preservation is often broad. Firebrand may preserve all email related to a specific topic, or all email for certain individuals.
In Exchange Online, you can use In-Place Hold or Litigation Hold to accomplish the following goals:

- Enable users to be placed on hold and preserve mailbox items immutably
- Preserve mailbox items deleted by users or automatic deletion processes such as MRM
- Protect mailbox items from tampering, changes by a user, or automatic processes by saving a copy of the original item
- Preserve items indefinitely or for a specific duration
- Keep holds transparent from the user by not having to suspend MRM
- Use In-Place eDiscovery to search mailbox items, including items placed on hold

Additionally, you can use In-Place Hold to:

- Search and hold items matching specified criteria
- Place a user on multiple In-Place Holds for different cases or investigations

DATA LOSS PREVENTION

The data loss prevention (DLP) feature will identify, monitor, and protect sensitive information in Firebrand through deep content analysis. DLP enables Firebrand to monitor business-critical email that includes sensitive data that needs to be protected. The DLP feature in Exchange Online enables Firebrand to protect sensitive data without affecting worker productivity.
Firebrand configure DLP policies in the Exchange admin center (EAC) management interface, which allows Firebrand to:

- Start with a pre-configured policy template that can help you detect specific types of sensitive information such as PCI-DSS data, Gramm-Leach-Bliley act data, or even locale-specific personally identifiable information (PII).
- Use the full power of existing transport rule criteria and actions and add new transport rules.
- Test the effectiveness of your DLP policies before fully enforcing them.
- Incorporate your own custom DLP policy templates and sensitive information types.
- Detect sensitive information in message attachments, body text, or subject lines and adjust the confidence level at which Exchange Online takes action.
- Detect sensitive form data by using Document Fingerprinting. Document Fingerprinting helps you easily create custom sensitive information types based on text-based forms that you can use to define transport rules and DLP policies.

Review incident data in DLP reports or add your own specific reports by using a generate incident report action.

ANTI-SPAM AND ANTI-MALWARE PROTECTION

Firebrand configures Microsoft Exchange Online that provides built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect our network from spam transferred through email. Firebrand Administrators do not need to set up or maintain the filtering technologies, which are enabled by default. However, administrators can make company-specific filtering customisations in the Exchange admin center (EAC).

ANTI-MALWARE PROTECTION

Using multiple anti-malware engines, Exchange Online offers multi-layered protection that's designed to catch all known malware. All messages transported through the service are scanned for malware (viruses and spyware). If malware is detected, the message is deleted. Notifications may also be sent to senders or administrators when an infected message is deleted and not delivered. We also choose to replace infected attachments with either default or custom messages that notify the recipients of the malware detection.

ANTI-SPAM PROTECTION

Exchange Online uses proprietary anti-spam technology to help achieve high accuracy rates. The service provides strong connection filtering and content filtering on all inbound messages. Outbound spam filtering is also always enabled if you use the service for sending outbound email, thereby helping to protect Firebrand using the service and their intended recipients.

QUARANTINE

Messages identified as spam and messages that match a transport rule can be sent to the administrator quarantine. Administrators can search for and view details about quarantined email messages in the EAC. After locating the email message, you can release it to specific users and optionally report it as a false positive (not junk) message to the Microsoft Spam Analysis Team if it was misidentified as spam.
There is also a spam quarantine for end users, which lets them manage their own spam-quarantined messages. End user management of spam-quarantined messages can also be performed via end-user spam notification messages.

ADDITIONAL PROCESSES AND PROCEDURES

- Audit policy for “access to data” falls in line with PCI compliance
- Systems and network segmentation reviewed frequently with a “needs must” policy.

Technologies and policies adhered to include:

- Boundary firewalls and internet gateways
    - Endpoint security controls
    - Firewall and security appliances
    - Group policy configuration
    - Proxy configuration for web browsing
    - VPN connectivity – Encryption and TFA
    - Azure trust centre
    - Hardware configuration documentation
    - Home working and mobile working policy
    - Monitoring
    - ACL Whitelist configuration for “safe” sites.
- Secure Configuration
    - Microsoft Group Policy configuration
    - Workstation build standards
    - Endpoint security configuration
    - Monitoring
    - Removable media control
- Access control and administrative privilege management
- Microsoft Group Policy configuration
    - Service accounts
    - Domain access accounts
- Endpoint security configuration
    - New user process
    - Malware protection
- Weekly review of Endpoint Protection reports
- Documentation of Endpoint Protection Configurations
- Patch management
    - Microsoft System Centre Operations Manager reports
    - Microsoft Windows Update Services reports
    - Microsoft Group Policy configuration for Windows Update
    - Request based software patching
- Cloud Hosted Systems
    - Cloud Trust Centre reports and configurations
- Physical Access Process and Policy
- Evidence of security polices
- Images of installed measures.

TRAINING & AWARENESS

All Staff are frequently reminded of best practice in relation to Cyber Security, and complete the Comptia CybserSecure Training course.
(https://cybersecure.org/pages/main)
***CompTIA CyberSecure is online cybersecurity training for everyone in the organisation. This self-paced training course teaches employees security best practices vital to protecting our business. The course focuses on implications of security behaviours of everyone in the workplace…not just the IT department. The 60-minute training covers online and offline behaviours that help reduce security risks.*
The Group IT & Security policy includes guidance on Cyber Security and is available to all staff to review within the company's HR portal.

Authorisation & Document Control

Document Title	Cyber Threat Policy			**Status**	V.1
Classification	Internal & External on	**Last Review**	September 2018	**Next Review**	June 2019
Location	Octopus Portal				

Authorisation	**Responsible Person or Body**
Document Owner	Gordon MacLeod (assisted by Dave Thompson, HR Consultant)
Authorised By	Gordon MacLeod

Version History

Version	**Author**	**Issued**	**Summary of Changes**
1.0	Gordon Macleod	09/06/17	First release