EXTREME FUNDING

1. Purpose

1.1. The purpose of this policy is to establish our organization’s responsibilities regarding corporate acquisitions and mergers. This policy also defines the minimum security requirements involved in the Information Security acquisition assessment.

2. Scope

2.1. This policy applies to all companies acquired by Extreme Funding and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company

2.2. The process of integrating a newly acquired company can have a drastic impact on the security posture of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

2.2.1. Assess company's security landscape, posture, and policies.

2.2.2. Protect both Extreme Funding and the acquired company from increased security risks.

2.2.3. Educate acquired company’s team members about Extreme Funding policies and standards.

2.2.4. Adopt and implement Extreme Funding Security Policies

2.2.5. Integrate acquired company

2.2.6. Continuous monitoring and auditing of the acquired company.

3. Policy Statements

3.1. General

3.1.1. Acquisition assessments are conducted to ensure that a company being acquired by Extreme Funding does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The Information Security Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Information Security role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work along with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to Extreme Funding's networks. Below are the minimum requirements that the acquired company must meet before being connected to the Extreme Funding network.

3.2. Hosts

3.2.1. All endpoints (servers, desktops, laptops) will be replaced or re-imaged with Extreme Funding standard security baseline configuration and will be required to maintain this minimum standards.

3.2.2. Business critical production servers that cannot be replaced or re-imaged must be audited. There must be an exception granted and documented by the Information Security Team.

3.2.3. All end-point computing devices will require Extreme Funding approved anti-virus protection and/or Endpoint Detection and Response software (EDR) before network connection is established.

3.3. Networks

3.3.1. All network devices will be replaced or re-imaged with a Extreme Funding standard baseline configuration.

3.3.2. Wireless network access points will be configured to the Extreme Funding standard baseline configuration.

3.3.3. The acquired company's network must comply with Extreme Funding network standard security baseline configuration.

3.4. Internet

3.4.1. All Internet connections will be terminated.

3.4.2. When justified by business requirements, air-gapped Internet connections will require the Information Security Team's review and approval.

3.5. Remote Access

3.5.1. All remote access connections will be terminated.

3.5.2. Remote access to any production, test, development, or guest network will be provided by Extreme Funding.

3.6. Labs

3.6.1. Lab equipment must be physically separated and secured from non-lab areas.

3.6.2. The lab network must be separated from the corporate production network with a Virtual network (VLAN) with a firewall between the two networks.

3.6.3. Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Information Security Team or the Lab Security Group (LabSec).

3.6.4. All acquired labs networks must conform with the LabSec standard security baseline configuration.

3.6.5. In the event the acquired networks and computer systems fail to meet these requirements, the Extreme Funding Chief Risk Officer (CRO) must acknowledge and approve of the risk to Extreme Funding's networks.

4. Responsibility

4.1. The Chief Information Security Officer of our organization or a designee from the Governance committee who will oversee and sign off on these Information Security policies. In smaller organizations, this may be the Information Security Manager. All employees, volunteers, and contractors are responsible for reading, understanding and complying with our organization's information security policies.

5. Compliance and Exceptions

5.1. The Information Security Team (InfoSec Team) will verify compliance to this policy through various methods, including but not limited to, reports from business tools, external audits, internal assessments, and interaction with the policy owner.

5.2. Any exception to the policy must be approved by the Infosec team in advance.

5.3. An employee, volunteer, or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination.

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a Extreme Funding-owned computer to remotely connect to Extreme Funding's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct Extreme Funding business must be approved in advance by InfoSec and the appropriate business unit manager.

4.1.5 All hosts that are connected to Extreme Funding internal networks via remote access technologies must use the most up-to-date anti-virus software (<place url to corporate software site here>), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

4.1.6 Personal equipment used to connect to Extreme Funding's networks must meet the requirements of Extreme Funding-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Extreme Funding Networks*.

1. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2. Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Extreme Funding's network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Third Party Agreement*
- *Hardware and Software Configuration Standards for Remote Access to Extreme Funding Networks*

All wireless infrastructure devices that reside at a Extreme Funding site and connect to a Extreme Funding network, or provide access to information classified as Extreme Funding Confidential, or above must:

4.1.1 Abide by the standards specified in the *Wireless Communication Standard*.
4.1.2 Be installed, supported, and maintained by an approved support team.
4.1.3 Use Extreme Funding approved authentication protocols and infrastructure.
4.1.4 Use Extreme Funding approved encryption protocols.
4.1.5 Maintain a hardware address (MAC address) that can be registered and tracked.
4.1.6 Not interfere with wireless access deployments maintained by other support organizations.

4.1 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to Extreme Funding Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the Extreme Funding network must:

4.2.1 Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the *Lab Security Policy*.
4.2.2 Not interfere with wireless access deployments maintained by other support organizations.

4.2 Home Wireless Device Requirements

4.3.1 Wireless infrastructure devices that provide direct access to the Extreme Funding corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

4.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Extreme Funding corporate network. Access to the Extreme Funding corporate network through this device must use standard remote access authentication.

1. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2. Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

6. Revision History

Date of Change	**Responsible**	**Summary of Change**
December 2022	Extreme Funding	Updated

Source: SANS