Terms and Conditions Policy

This page was last changed on 2 May 2024, last checked on 2 May 2024 and applies to all users of this website.

Acceptable Use

. Personnel are responsible for complying with Lonestar Valor Funding policies when using Finch
Model information resources and/or onLonestar Valor Funding time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.

• Personnel must promptly report harmful events or policy violations involving Lonestar Valor Funding assets or information to their manager or a member of the Incident Handling
Team. Events include, but are not limited to, the following:

• Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Finch Model **Information Resources**.
• Data incident: any potential loss, theft, or compromise of Lonestar Valor Funding information.
• Unauthorized access incident: any potential unauthorized access to a Lonestar Valor Funding **Information Resource**.
• Facility security incident: any damage or potentially unauthorized access to a Lonestar Valor Funding owned, leased, or managed facility.
• Policy violation: any potential violation of this or other Lonestar Valor Funding policies, standards, or procedures.

•Personnel should not purposely engage in activities that may
• harass, threaten, impersonate, or abuse others;
• degrade the performance of Finch Model **Information Resources**;
• deprive authorized Finch Model personnel access to a Lonestar Valor Funding **Information Resource;**
• obtain additional resources beyond those allocated;
.• or circumvent Lonestar Valor Funding computer security measures.

Personnel should not download, install, or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Lonestar Valor Funding personnel

• should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Finch Model **Information Resource**.
All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical

• information, developed on Lonestar Valor Funding time and/or using Finch Model **Information**

.**Resources** are the property of Lonestar Valor Funding.
Use of encryption should be managed in a manner that allows designated Lonestar Valor

•Funding
personnel to promptly access all data.

Finch Model **Information Resources** are provided to facilitate company business and should not be used for personal financial gain.

Personnel are expected to cooperate with incident investigations, including any federal or state investigations.

- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Lonestar Valor Funding **Information**
- **Resources**.
  Personnel should not intentionally access, create, store or transmit material that Finch Model may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "**need-to-know basis**".
- Personnel are permitted to use only those network and host addresses issued to them by Lonestar Valor Funding IT and should not attempt to access any data or programs contained on Lonestar Valor Funding systems for which they do not have authorization or
- explicit consent.
  All remote access connections made to internal Lonestar Valor Funding networks and/or environments must be made through approved, and provided, virtual private networks
- (VPNs).
  Personnel should not divulge any access information to anyone not specifically
- authorized to receive such information, including IT support personnel.
  Personnel must not share their personal authentication information, including:

  • Account passwords,
  • Personal Identification Numbers (PINs),
  • Security Tokens (i.e. Smartcard),
  • Multi-factor authentication information
  • Access cards and/or keys,
  • Digital certificates,
  • Similar information or devices used for identification and authentication
- purposes.
  Access cards and/or keys that are no longer required must be returned to physical
- security personnel.
  Lost or stolen access cards, security tokens, and/or keys must be reported to physical
- security personnel as soon as possible.
  A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following Lonestar Valor Funding rules:

  • Must meet all requirements including minimum length, complexity, and reuse history.
  • Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
  • Must not be the same passwords used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone. Finch Model support personnel and/or contractors should never ask for user account passwords.

- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard-coded passwords in client software.
- Security tokens (i.e. Smartcard) must be returned on demand or upon the termination of the relationship with Finch Model, if issued.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Physical and/or electronic keys used to access **confidential information** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing **confidential information** should be immediately removed from printers and fax machines.

Data Security

- Personnel should use approved encrypted communication methods whenever sending **confidential information** over public computer networks (Internet).
- **Confidential information** transmitted via USPS or other mail service must be secured in compliance with the Information Classification and Management Policy.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- **Confidential information** must be transported either by a Lonestar Valor Funding employee or a courier approved by IT Management.
- All electronic media containing confidential information must be securely disposed of. Please contact IT for guidance or assistance.

Email and Electronic Communication

- Auto-forwarding electronic messages outside Finch Model internal systems is prohibited.
- Electronic communications should not misrepresent the originator or Finch Model.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from Finch Model IT, except for calendars and related calendaring functions with express permission.
- Employees and anyone directly working for (in any capacity) Finch Model should not use personal email accounts to send or receive Finch Model **confidential information**.
- Any personal use of Finch Model provided email should not:

- Involve solicitation.
- Be associated with any political entity, excluding Finch Model sponsored PAC.
- Have the potential to harm the reputation of Finch Model.
- Forward chain emails.
- Contain or promote anti-social or unethical behaviour.
- Violate local, state, federal, or international laws or regulations.
- Result in unauthorized disclosure of Finch Model **confidential information**.
- Or otherwise violate any other Finch Model policies.

- Personnel should only send **confidential information** using approved secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing **confidential** or **internal information** in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to Finch Model networks.
- Software installed on Finch Model equipment must be approved by IT Management and installed by Finch Model IT personnel.
- All Finch Model assets taken off-site should be physically secured at all times.
- Personnel travelling to a High-Risk location must contact IT for approval to travel with corporate assets.
- Personnel (regardless of capacity) should not allow family members or other non-employees to access Finch Model **Information Resources**.

Internet

- The Internet must not be used to communicate Finch Model **confidential** or **internal information** unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with Finch Model networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
  - Recreational games,
  - Streaming media,
  - Personal social media,
  - Accessing or distributing pornographic or sexually oriented materials,
  - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
  - Or otherwise violate any other Finch Model policies.
- Access to the Internet from outside Finch Model network using a Finch Model owned computer must adhere to all of the same policies that apply to use from within Finch Model facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- The use of a **personally owned mobile device** to connect to Finch Model network is a privilege granted to employees only upon formal approval of IT Management.
- All **personally owned** laptops and/or workstations must have approved and active virus and spyware detection/protection software along with personal firewall protection.
- Mobile devices that access Finch Model email must have a PIN or other authentication mechanism enabled.
- **Confidential information** should only be stored on devices that are encrypted in compliance with Finch Model Encryption Standard.
- Finch Model **confidential information** should not be stored on any personally owned **mobile device**.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to Finch Model Security Team immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** ethically.
- **Jail-broken** or rooted devices should not be used to connect to Finch Model **Information Resources**.
- Finch Model IT Management may choose to execute "**remote wipe**" capabilities for **mobile devices** without warning (see Mobile Device Email Acknowledgement).
- If there is a suspected **incident** or breach associated with a **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage concerning Finch Model **Information Resources** may be monitored, at the discretion of Finch Model IT Management.
- Finch Model IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. Finch Model IT support may not assist in troubleshooting device usability issues.
- Use of **personally owned** devices must comply with all other Finch Model Policies and Procedures.
- Finch Model reserves the right to revoke **personally owned mobile device** use privileges if personnel do not abide by the requirements outlined in this policy.

Privacy

- Information created, sent, received, or stored on Finch Model **Information Resources** is not private and may be accessed by Finch Model at any time, under the direction of Finch Model executive management, without knowledge of the user or resource owner.
- Finch Model may log, review, and otherwise utilize any information stored on or passing through its **Information Resource**
- Systems Administrators, Finch Model IT, and other authorized Finch Model personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment-related task.

Removable Media

- The use of **removable media** for storage of Finch Model information must be supported by a reasonable business case.
- All **removable media** use must be approved by Finch Model IT prior to use.

- **Personally, owned removable media** use is not permitted for storage of Finch Model
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from Finch Model
- Confidential and internal Finch Model information should not be stored on **removable media** without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a **removable media** device that may have contained any Finch Model information must be reported to Finch Model

Security Training and Awareness

- All new personnel must complete an approved **security awareness** training class prior to, or at least within 30 days of, being granted access to any Finch Model **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to Finch Model Information Security Policies before they are granted access to Finch Model **Information Resources**.
- All personnel must complete the annual security awareness training.

Social Media

- Communications made concerning social media should be made in compliance with all applicable Finch Model Policies and Procedures.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Finch Model, including accounts that could reasonably be assumed to be an official Finch Model account, requires the permission of Finch Model Communications Departments.
- When discussing Finch Model or Finch Model-related matters, you should:
  - Identify yourself by name,
  - Identify yourself as a Finch Model representative (provided that you have been approved as such), and
  - Make it clear that you are speaking for yourself and not on behalf of Finch Model unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at Finch Model.
- When publishing Finch Model-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent Finch Model’s position or opinion.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, colour, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with Finch Model will not be tolerated.
- **Confidential information**, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on Finch Model social media sites must follow Finch Model Social Media Management Procedures.

VoiceMail

- Personnel should use discretion in disclosing **confidential** or **internal information** in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- Personnel should not access another user's voicemail account unless it has been explicitly authorized.
- Personnel must not disclose **confidential** information in voicemail messages.

Incidental Use

- As a convenience to Finch Model personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:
  • Storage of personal email messages, voice messages, files and documents within Finch Model **Information Resources** must be nominal
  • All information located on Finch Model **Information Resources** are owned by Finch Model may be subject to open records requests and may be accessed in accordance with this policy.

Waivers

Waivers from certain policy provisions may be sought following Finch Model Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.