NS CAPITAL LLC
The New Standard in Portfolio Management

2022 Cyber Security Policy

Policy brief & purpose

NS Capital's cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors and anyone who has permanent or temporary access to our systems and hardware ("employee").

Policy elements

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data by following the below listed required guidelines:

1. Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We require our employees to keep both their personal and company-issued computer, tablet and cell phone secure with the following protocol:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

Additionally, we prohibit employees from accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment, such equipment is added to the current 3rd party monitoring system and the appropriate anti-malware/anti-virus protection applications downloaded directly into the device. Questions regarding the safety of both personal and company-issued equipment may be directed to Eric P. Hahn, our internal technology coordinator (ITC).

2. Keep emails safe

Emails often host scams and malicious software (e.g. worms) To avoid virus infection/data theft, we require employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive punctuation, etc.)

If an employee isn't sure that an email they receive is safe, they can refer to the ITC or the HR Manager (Beverly Blair); ***but under no circumstances should an Employee click on an uncertain link or call-to-action.***

3. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we require our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

4. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask the ITC for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or non-employee private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts
- Password protect any data containing confidential data, and relay password by alternate communication.

Our ITC needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we insist our employees report perceived attacks, suspicious emails or phishing attempts as soon as possible. Our ITC must investigate promptly, resolve the issue and send a company-wide alert when necessary.

5. Additional measures & 3rd-Party services

To reduce the likelihood of security breaches, we also require our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to the ITC or HR Manager.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy which strictly prohibits company-issued equipment from accessing questionable or unstable sites.

Our ITC and 3rd-party IT Monitoring providers work in conjunction to provide the following supplemental measures to our internal IT security protocol:

- Manage virtual firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Monitor the system for continual and relevant updates to core systems and patches, applications and proprietary software.
- Implement a fully restored recovery system to mitigate "down time" during breaches.

6. Remote employees

Remote employees must follow this Cyber Security Policy as well as stationed employees. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage them to seek advice from our ITC if there is a chance their security measures do not meet our standards or they need assistance in properly securing their equipment.

7. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- *First-time, unintentional, small-scale security breach:* We may issue a verbal warning and train the employee on security.
- *Intentional, repeated or large-scale breaches (which cause severe financial or other damage):* We will invoke more severe disciplinary action up to and including termination and/or legal action.
- We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

8. Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Questions regarding these policies or doubt concerning the security of a particular communication or action should be referred to either Eric P. Hahn or Beverly Blair.

Note: This Cyber Security Policy applies to NS Capital LLC, an independent, privately owned, fee-only Registered Investment Advisory Firm. NS Capital reserves the right to change this Cyber Security Policy at any time, without notice and update any amended version of this document to this website.