Nomad Cuts IT Security Policy

Table of Contents

Nomad Cuts Access Control Policy

Effective Date: 4/11/2025

Enterprise or Departmental: Enterprise

Approved: Yes

Policy Revision #: 1.0

Access Control Policy

Purpose

The intent of this policy is to define the Nomad Cut's requirement for providing employees, users, authorized third parties, and system administrators with access to systems, applications, and data. Given the Nomad Cuts's Data Classification Policy, role-based access controls will be defined for each job function. Each job description will have job tasks and functions defined that may require access to systems, applications, and data. Depending on the sensitivity of the job function, access to sensitive data may be required.

Scope

This IT Security Policy applies to all digital assets, users, and systems involved in the operation of Nomad Cut's mobile haircut service. This includes:

Customer-Facing Platforms:

- Mobile apps (iOS and Android)
- Web portal for booking services
- Online payment and scheduling systems

Internal Systems:

- Staff management platforms
- Customer relationship management (CRM) tools
- Business email and communication tools
- Cloud-hosted infrastructure and databases

User Types Covered:

- Employees (e.g., support staff, managers)

- Contractors (e.g., mobile hair stylists)
- Third-party vendors (e.g., app developers, payment processors)
- Customers who use the platform to schedule appointments

Devices and Networks:

- Company-issued and personal mobile devices used by stylists and staff
- Secure connections to backend systems and databases
- Wi-Fi and mobile networks used to access the platform

This policy governs the access, handling, and protection of sensitive data such as customer names, addresses, phone numbers, appointment history, and payment information. It ensures that all users and systems are aligned with data privacy best practices and regulatory standards.

The operational and management scope of this Access Control Policy shall include:

- Authorization- New hire, HR onboarding, and role-based access control are defined.
- Identification- Unique login ID is provided
- Authentication- Temporary password is provided requiring the user to change to complex and very strong password
- Accounting- Audit trails, logs, and user additions and deletions

Policy

All employees, authorized users, and authorized third parties shall be granted access to the Nomad Cuts network, systems, applications, and data as needed to perform their job responsibilities.

The following defines the security controls for access controls:

- Onboarding must be completed prior to the new hire obtaining their login credentials
- Access privileges are determined based on the least necessary to perform job responsibilities
- Access is granted based on job role
    - Customers
    - Stylists
    - Admins (Managers, HR)
- Each employee will be assigned a unique user ID and password for the following:
    - Access to the Nomad Cut’s workstation/laptops
    - Role-based access to the systems, applications, and data required of the job responsibilities
- Users are not to share their usernames or passwords
- Users are to abide by the Nomad Cut’s password management standard requiring the user to have the following password requirements:
    - 8 characters at least

    - At least one capital
    - At least one number
    - At least one symbol
    - Password must not be reused
- Alpha-character names or numbers that have meaning to the individual are not permitted to be used (e.g., names of children or pets, birth year, graduation year, street address number, etc.).
- Passwords must be changed every 90 days
- Users must have Multi-Factor Authentication (MFA) for Admin access
- System administrators shall have proper separation of duties providing hierarchical privileged access to the network, systems, and applications and different functions.

Noncompliance or Policy Violations

Noncompliance with this policy definition will be monitored, tracked, and handled by the Human Resources department, the employee's department head, and the Information Technology department.

All employees, authorized users, and authorized third parties that are in violation of this policy will be required to work with the Human Resources department and the Information Technology department.

Revisions

Revision Date (MM/DD/YYYY)	Author	Description of Changes

Nomad Cuts Acceptable Use Policy

Effective Date: 4/11/2025

Enterprise or Departmental: Enterprise

Approved: Yes

Policy Revision #: 1.0

IT Acceptable Use Policy

Purpose

This policy shall define acceptable use of Nomad Cut's IT assets, Internet, email, systems, applications, and data. This policy shall also define unacceptable use.

Scope

The scope of this enterprise-wide policy encompasses the entire organization and all employees, authorized users, and authorized third parties who are granted access controls to the IT infrastructure.

All employees, contractors, and authorized third parties that are provided with a login ID and password must comply with this acceptable use policy. This policy mandates that all employees, contractors, and authorized third parties taker special precautions as they pertain to the access, use, handling, storage, and transmission of sensitive data as part of normal day-to-day operations and business functions.

Acceptable Use Policy

Policy

All authorized users (employees, contractors, or authorized third parties) that require access to the Nomad Cuts IT assets, systems, applications, and data must read, acknowledge, and sign this Acceptable Use Policy prior to being granted login credentials

Most importantly this policy shall define what is acceptable use and what is not acceptable use of the Nomad Cut's owned IT systems, applications, and data.

Acceptable Use

- Us provided computer equipment, hardware, and software applications to do your job functions and tasks only.
- Protect login credentials and use strong passwords
- Lock or log out of devices when unattended

- Ensure that no sensitive data is screen captured or cut and pasted into separate or stand alone documents or saved to unapproved data devices.
- External storage media must use encrypted or password protected files.
- Keep software and applications up-to-date and patched
- Use only devices that have been approved by the organization for business functions.

Unacceptable Use

- Sharing login credentials or using another user's account
- Accessing, copying, or modifying customer or company data without authorization
- Using company platforms for unauthorized commercial or personal purposes
- Downloading or installing unapproved apps, tools, or browser extensions
- Accessing systems from unsecured or public Wi-Fi without a VPN
  Storing business data on unauthorized personal devices or cloud storage
- Attempting to disable or bypass security settings or controls
- Sharing sensitive company or customer information on social media or public forums

Noncompliance or Policy Violations

Noncompliance with this policy definition will be monitored, tracked, and handled by the Human Resources department, the employee's department head, and the Information Technology department.

Any employees or authorized users that are in violation of this policy will be required to work with the Human Resources department for remediation.

This remediation effort may include review of the Nomad Cut's policies and procedures, or other disciplinary actions.

Acknowledgement

Employee

Name: _____

Signature: _____

Title: _____

Date: _____

Supervisor

Name: _____

Signature: _____

Title: _____

Date: _____

Human Resources

Name: _____

Signature: _____

Title: _____

Date: _____

Revisions

Revision Date (MM/DD/YYYY)	Author	Description of Changes

Nomad Cuts Data Classification Policy

Effective Date: 4/11/2025

Enterprise or Departmental: Enterprise Policy

Approved: Yes

Policy Revision #: 1.0

Data Classification Policy

Purpose

The intent of this policy is to provide the organization with a consistent definition for different classes of information. Once defined all employees and users will access, use, handle, process, store, and transmit data consistently according to its classification. This is important given the sensitive data used by the organization.

Scope

The scope of this enterprise-wide policy includes all employees, authorized users, and third parties who are granted access to the Nomad Cuts systems, applications, and data.

Policy

Classification Level	**Description**
Level 1- Low Public Domain Low Sensitivity	Data in this classification can be accessed and shared with the general public. No labeling or security controls are required when handling this category of data. Data classification in this category shall include but is not limited to: • Company website content • Service descriptions • Pricing for public services • Job postings • Business hours and locations • Social media posts • Approved marketing materials

Level 2- Medium Internal Business Use Only Medium Sensitivity	Data in this classification shall be treated as confidential, Internal Business Use Only to be shared only with authorized users between the Nomad Cut's departments and employees. • Internal emails and team messages • Meeting notes and schedules • Employee handbooks or training materials • Appointment logs (without sensitive customer info) • Vendor contact lists • Non-confidential business strategies
Level 3- High Sensitivity	This classification is for the most sensitive data used, handled, stored, and/or transmitted throughout the Nomad Cuts network infrastructure and work environment. • Customer personally identifiable information (PII) (e.g., full names, addresses, phone numbers) • Payment information (e.g., credit/debit card data) • Login credentials and password data • Employee personal and payroll records • Security logs and incident reports • Business financials and private contracts • Proprietary algorithms or source code

Minimum Sensitivity Levels

The table below summarizes types of data utilized and stored throughout the network infrastructure by the organization and lists the minimum sensitivity level of these data categories or types. This can be used as a guideline for classifying other forms of data that new applications may use, handle, store, or transmit.

Data Category	Description	Minimum Classification Level
Investigative or Intelligence	Data under attorney-client privileged communications. Data/Information related to investigations, law enforcement, subpoenas, court cases, and special operational activities.	3
Legal, Law Enforcement, and Emergency Response	Data/information related to legal, law enforcement activities, or emergency response that would adversely impact the organization	3

	or individuals involved if released.	
Financial Data of Customers or the Organization	Customer or organization financial data that: a) Is created or received by an employee b) Shall be fully encrypted in transmission; isolated from the rest of the Nomad Cuts network infrastructure	3
Personally Identifiable Information (PII) Data Subject to Privacy Laws	Any item, collection, or grouping of data/information about a U.S. citizen or permanent resident employed by the organization	3
Emergency Operations and Procedures (BIA, BCP, DRP, and CSIRT Plan)	Information related to the Nomad Cuts IT security posture, including automated data processing security, internal operations, workflows, security controls, and risks, threats, and vulnerabilities.	3
Financials, Business Workflows	Information related to the Nomad Cuts business partners, vendors, and contractors financials, taxes, revenue, accounting or commercial activities, business workflows, procurement, and any other nonexempt data.	2
Personnel	Data/Information whose external or internal release would have a negative impact on an individual	2
Internal Data for Business Use Only	Memos, spreadsheets, and documents containing general organizational business operations and information that would not be made generally available to the public.	2
External Data that is Considered Public Domain	Emails, memos, spreadsheets, SMS text messages, and documents containing general information that is not covered under Level 3 or Level 2 data classification definitions. This classification of data can be found in the public domain or can be	1

	shared in the public domain with no adverse effect or risk exposure to the organization.	

Noncompliance or Policy Violations

Noncompliance with this policy will be monitored, tracked, and handled by the Nomad Cuts Information Technology department and Human Resources department.

The Information Technology department and each department head shall be held responsible and accountable for enforcing this policy throughout.

Resources, tools, and defined procedures are the responsibility of the Information Technology department, and each application owner and/or data owner assigned.

Approval

Executive or Board Level Review & Approval

Name: _____

Title: _____

Signature: _____

Date: _____

Revisions

Revision Date (MM/DD/YYYY)	Author	Description of Changes

Nomad Cuts Network Security Policy

Effective Date: 4/11/2025

Enterprise or Departmental: Enterprise Policy

Approved: Yes

Policy Revision #: 1.0

Network Security Policy

Purpose

The intent of this policy is to provide the Nomad Cut's Information Technology department with a clear and concise definition of why, where, and how to implement network security controls.

Scope

This policy applies to all employees, contractors, and authorized third party users who access or manage:

- Internet and wireless networks used for company operations
- Servers, firewalls, and routers
- Company laptops, mobile devices, and any device connected to the company network
- Cloud platforms or third-party services that transmit or store company data

It covers both physical and cloud-based network components used for internal operations and customer-facing services.

Policy

This Network Security Policy requires the Information Technology department to build baseline definitions to ensure the confidentiality, integrity, and availability of system and network resources.

- Design and implement a closed internal IP data networking environment
- Design and implement segmented physical and logical IP data networking environment using IEEE 802. IQ Layer 2,, virtual LAN technology
- Design and implement Layer 3 backbone networks where alternate routes are needed for the IP data network infrastructure to achieve a 99.5% uptime
- No unauthorized connections to the organizations IP data network are permitted. Any rouge devices will be removed from the network.
- Nomad Cuts has the right to audit and monitor all network connections and n network traffic initiated by the employees, users, and authorized third parties.

Noncompliance or Policy Violations

Noncompliance with this policy will be monitored, tracked, and handled by the Nomad Cuts Information Technology department

Approval

Executive or Board Level Review & Approval

Name: _____

Title: _____

Signature: _____

Date: _____

Revisions

Revision Date (MM/DD/YYYY)	Author	Description of Changes