



Brand Guidelines

2024

WHERE **TECHNOLOGY**
MEETS **TRUST**



Contents

01 Mission	4
02 Brand Values	6
03 Identity	8
Tagline	9
Logo	10
Logo Usage	11
Colors	14
Typography	16
Pattern	17
04 Product Segments	18

01 Mission



Empowering a Secure, Connected World through Digital Innovation

Our mission is critical because we secure everything from the White House to public schools, making the physical world more secure and responsive.

Hirsch is a global technology leader specializing in physical security solutions, video intelligence, and digital identification systems.

Dedicated to continuously innovating and securing a connected world, we provide comprehensive cybersecurity and the full spectrum of physical access, video, and logical access solutions. We verify frictionless access and anywhere operations, protect identities from malicious attacks, secure intellectual property, and drive innovation. We digitally secure the physical world.

02 Brand Values



Hirsch stands for **Authenticity, Innovation,** and **Trust** in technology.

> **AUTHENTIC**

We use clear language to make technology accessible to everyone, experts to beginners. We are straightforward and easy to understand.

> **INNOVATIVE**

The stories we tell inspire others to think, engage, and create. We are technology futurists building for the world of today but thinking of tomorrow.

> **TRUSTED**

We are a global leader in physical security and digital identity solutions, bringing 43 years of industry experience. We are accessible and audience-focused.

WHAT MAKES HIRSCH DISTINCTIVE:

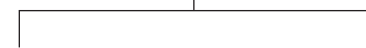
- 1. Holistic Security Expertise:** From securing high-profile government buildings to public schools, Hirsch's comprehensive suite of solutions makes both the digital and physical worlds more secure and responsive.
- 2. Human-Centric Technology:** Our focus isn't just on creating technology but on making it usable and beneficial for people. We simplify complex solutions, making them accessible to all, from experts to beginners.
- 3. Trusted Partnership:** More than a vendor, we serve as a trusted technology partner to our customers. With over 43 years of industry experience, we've earned a reputation for reliability, authenticity, and innovation.
- 4. Global Reach, Local Impact:** With operational centers across the globe and partnerships in various sectors, our impact is international, yet our solutions are tailored to meet local and specific industry needs, from community centers to hospitals.

03 Identity

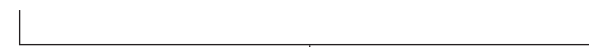


Tagline

Montserrat Regular



WHERE **TECHNOLOGY** MEETS **TRUST**



Montserrat Bold

Logo

Horizontal Layout



Vertical Layout



Horizontal Layout with Tagline



Vertical Layout with Tagline



The Hirsch logo is the heart of our identity. It is the first way we connect to our customers. We must use it correctly everywhere it appears.

Logo Usage

Size



Any logo usage below 1.5" must use logos noted "Below 1.5in" in file name. This logo increases character leading for readability

Minimum Size

PRINT



SCREEN



Clear Space



What is clear space? It is the area surrounding the logo. Clear space must be kept free of any text or graphic elements.

By leaving ample space around the logo, we make sure the logo stands out.

Clear space is measured by the x-height of the Hirsch letters, shown as "X" in this exhibit. The minimum clear space must always be 1X on all sides of the logo. When possible, this amount should be increased for even more visibility.

Logo Usage

Color Specification

Positive logos may be placed on backgrounds up to 20% tint



20% tint

Red and White logos may be placed on Dark backgrounds



White logo may be placed on red backgrounds



White logo may be placed on dark photographic backgrounds



Logo Usage

Logo Do NOT's



Change the logo's orientation or rotation



Disproportionately scale or resize the logo



Use the logo on dark colors



Use the logo on top of busy photography



Use the red logo on red backgrounds



Violate the logo clear space

Colors

Primary Colors

CMYK 15 100 100 55

RGB 114 2 3

HEX #720203

PMS 188 C

CMYK 10 100 100 30

RGB 163 20 24

HEX #a31418

PMS 187 C

CMYK 0 100 100 10

RGB 215 25 32

HEX #d71920

PMS 186 C

CMYK 0 0 0 75

RGB 99 100 102

HEX #636466

PMS Cool Gray 9 C

CMYK 0 0 0 45

RGB 157 159 162

HEX #9d9fa2

PMS Cool Gray 6 C

Colors

Secondary Colors

CMYK 100 92 38 38

RGB 25 36 78

HEX #19244e

PMS 281 C

CMYK 90 51 9 0

RGB 0 115 174

HEX #0073ae

PMS 2925 C

CMYK 52 13 0 9

RGB 105 170 212

HEX #69aad4

PMS 291 C

CMYK 0 25 90 10

RGB 230 177 46

HEX #e6b12e

PMS 1225 C

Typography

HEADLINES

Montserrat Bold

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz 0123

SUBHEADLINES

Montserrat Bold

ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123

BODY TEXT

Montserrat Light

ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123

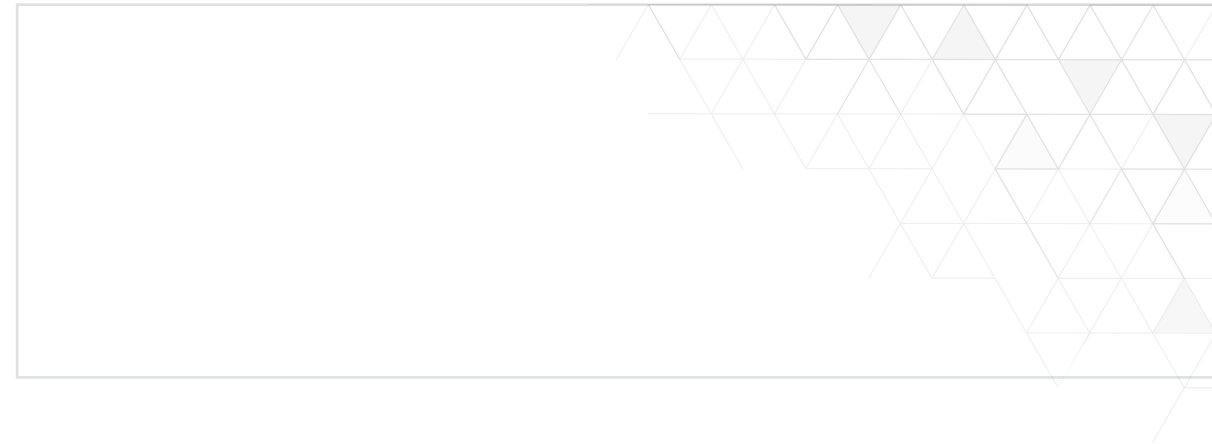
LEGAL TEXT

Montserrat Light

ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123

Pattern

Positive Gray patterns can be placed on White backgrounds



Negative White patterns can be placed on Color backgrounds



04 Product Segments



Premises

SECURE. PREVENT. DETECT. PROTECT.

Enhance your security backbone with Hirsch's award-winning, trusted physical security capabilities. Discover end-to-end, feature-rich physical access control, video intelligence, and credentialing solutions that fit your unique business needs.

Hirsch's physical access control, video intelligence, and identification solutions provide the highest security at the lowest cost. Robust, feature-rich systems, hardware, and software verify frictionless access managed from anywhere. Highly secure credentials, IDs, and smart cards identify employees, temporary workers, and visitors in a wide range of form factors and frequencies.

Hirsch credentials, IDs, and smart cards verify the identity of employees, temporary workers, and visitors. Our portfolio features form factors for physical or logical access control, converged access, transit payment, brand protection, time and attendance, cashless vending, and IoT applications.

Color Palette



Marketing Style

HIRSCH
Title Title Title
Subtitle subtitle

Hirsch Velocity Cirrus is a secure, cloud-based solution available from any computer, anytime, anywhere.

Velocity Cirrus manages access control and security operations from single high-secure rooms to multi-building, multi-location campuses. Control doors, gates, turnstiles, elevators, and other building equipment, monitor users moving around a facility, prevent unwanted access, maintain compliance, and provide a robust audit trail.

As a hosted Access Control as a Service (ACaaS) solution, it is always maintained on the latest iteration of Identiv's world-class physical access software platform without the need to ever upgrade or apply patches.

It delivers unsurpassed security, interoperability, and greater expansion and flexibility options designed to accommodate the evolution of security technology while meeting the needs of even the most complex business, personnel, and facility requirements.

Designed and built from the ground up, it provides full compatibility with the latest hardware in the Mix Controller product line and supports the latest versions of Microsoft Windows and SQL Server and supports the latest network of encryption protocol (TLS).

Advanced Features

- Government-grade, secure connectivity between hardware and server, A/B rules, two-person rules, and anti-passback

Cloud-Based Access

- Users no longer need to manage local software or server hardware

True Portability

- Offers benefits of high-availability, infinite-scalability, cybersecurity technology

Future-Proof

- Lower costs, lower maintenance, and the assurance of always having the latest version

HIRSCH DATA SHEET Title Title Title
Sub title sub title sub title

Features

- Controls one (1) fully supervised door with entry and optional exit keypad/readers or eight (8) wireless door locks
- Scalable from single controller to networked multi-site installations
- Multi-microprocessor architecture with dedicated crypto-processor
- Integrated network communication with onboard 10/100/1000 Ethernet IP port
- Auxiliary alarm relay output
- Integrated hardware encryption with enabled devices
- High-security supervised alarm inputs
- Configurable relay outputs (door or general purpose)
- Open Secure Device Protocol (OSDP)
 - ScramblePads, TS readers, and third-party OSDP readers (i.e., VeriD Stealth Series)
 - Reader LED and buzzer control
 - Extended cable runs
 - Entry/exit reader setup
- Supports Wiegand readers
- Global UID
- Firmware can be updated through Velocity
- Powered at the edge by PoE+ or external power supply
- Special circuitry to protect reader/relay terminals from excessive current draws
- Supports a wide variety of readers and credentials
- Built-in protection from door strikes and mag locks that generate large inrush current demand during power-up and large induced current demand during power-down

Intelligent Distributed Architecture

Access may be restricted based on Time of Day, Day of Week, and Door. Access may be granted when the user presents the correct code, card, or both. The user may be granted temporary access based on Use Count Limits, Temporary Day Limits, and Absentee Rule Limits, with Auto-Disable or Auto-Delete on Expiration of Temporary Users. Additional functions include Unlock/Relock, Alarm Mask/Unmask, and Lock Down/Lock Down Release. The associated door may be monitored for Door Forced Open and Door Open Too Long, while providing Auto Relock Control.

High Security Alarm Monitoring

Identiv uses very stable digitally processed analog inputs with line supervision for high-security alarm monitoring. A line supervision module is located at the door contact, alarm sensor, request to exit (RQE), or similar device to establish this supervision. Conditions reported include Alarm, Secure, RQE, Mask, Tamper Alarm, Tamper Secure, Short, Open, Noisy, and Input-Out-of-Spec.

Reliability by Design

Mx1 Controllers are designed for high availability as a complete system for global markets. A standby battery for memory is standard, while a standby UPS or battery for operation is optional. The controller ships ready to be connected to a PoE+ power source, and has support for optional external power supplies. Power connectors are fused. Readers and relays are protected by built-in hardware circuits which will cut off power when they detect over-power consumption, protecting the board against unintended damage.

Features and Benefits

The Mx1 has a built-in Secure Network Interface Board 3 (SNIB3) with enhanced memory storage at 500K credentials, security, TLS, 128-bit, or 256-bit encryption options, and network functionality and capabilities. The SNIB3 is a leading edge communication device that provides IPv4, Gigabit Ethernet, and IEEE 802.3 certified cryptography, including AES 256.

hirschsecure.com • sales@hirschsecure.com • +1 888-809-8880
Hirsch is part of the VeriGroup Group.

HIRSCH DATA SHEET Title Title Title
Sub title sub title sub title

Cirrus Network Installation Diagram

Contact Information

Optimize your Identiv product implementation and support efforts with professional project management. Ensure efficiency, reduce risks, and maintain high-quality support services to achieve successful product deployments.

For inquiries, pricing, and technical support, please contact us at:

HIRSCH
TECHNICAL DATA IS SUBJECT TO CHANGE WITHOUT NOTICE. REVISION DATE: 2025-07-15
Hirsch is a global technology leader, revolutionizing physical security, video intelligence, and digital identification systems. Hirsch is part of the VeriGroup Group. For more information, visit hirschsecure.com or email info@hirschsecure.com.
© Hirsch, Inc. All rights reserved. This document is Hirsch proprietary information.

YOUR WORLD, **VERIFIED.** YOUR IDENTITY, **SECURED.**

Identity

Hirsch's multi-factor authentication solutions help organizations remain trusted and deliver outstanding employee and customer experiences without worrying about cybersecurity or compromised digital identities.

Hirsch's logical access control technology identifies and verifies users to safely and securely access data. Remote and multi-factor authentication (MFA) and embedded application solutions protect data on-the-go, in the office, or at home.

Color Palette



Marketing Style

HIRSCH
Title Title Title
Subtitle subtitle

Hirsch Velocity Cirrus is a secure, cloud-based solution available from any computer, anytime, anywhere.

Velocity Cirrus manages access control and security operations from single high-secure rooms to multi-building, multi-location campuses. Control doors, gates, turnstiles, elevators, and other building equipment, monitor users moving around a facility, prevent unwanted access, maintain compliance, and provide a robust audit trail.

As a hosted Access Control as a Service (ACaaS) solution, it is always maintained on the latest iteration of Identity's world-class physical access software platform without the need to ever upgrade or apply patches.

It delivers unsurpassed security, interoperability, and greater expansion and flexibility options designed to accommodate the evolution of security technology while meeting the needs of even the most complex business, personnel, and facility requirements.

Designed and built from the ground up, it provides full compatibility with the latest hardware in the Mx Controller product line and supports the latest versions of Microsoft Windows and SQL Server and supports the latest network of encryption protocol (TLS).

Advanced Features

- Government-grade, secure connectivity between hardware and server, A/B rules, two-person rules, and anti-passback

Cloud-Based Access

- Users no longer need to manage local software or server hardware

True Portability

- Offers benefits of high-availability, infinite-scalability cybersecurity technology

Future-Proof

- Lower costs, lower maintenance, and the assurance of always having the latest version

Government-grade, secure connectivity between hardware and server, A/B rules, two-person rules, and anti-passback

Users no longer need to manage local software or server hardware

Offers benefits of high-availability, infinite-scalability cybersecurity technology

Lower costs, lower maintenance, and the assurance of always having the latest version

HIRSCH DATA SHEET
Title Title Title
Subtitle subtitle subtitle

Features

- Controls one (1) fully supervised door with entry and optional exit keypad/readers or eight (8) wireless door locks
- Scalable from single controller to networked multi-site installations
- Multi-microprocessor architecture with dedicated crypto-processor
- Integrated network communication with onboard 10/100/1000 Ethernet IP port
- Auxiliary/Alarm relay output
- Integrated hardware encryption with enabled devices
- High-security supervised alarm inputs
- Configurable relay outputs (door or general purpose)
- Open Secure Device Protocol (OSDP)
 - ScramblePads, TS Readers, and third-party OSDP readers (i.e., Verifi Stealth Series)
 - Reader LED and buzzer control
 - Extended cable runs
 - Entry/Exit reader setup
- Supports Wiegand readers
- Global UID
- Firmware can be updated through Velocity
- Powered at the edge by PoE+ or external power supply
- Special circuitry to protect reader/relay terminals from excessive current draws
- Supports a wide variety of readers and credentials
- Built-in protection from door strikes and mag locks that generate large inrush current demand during power up and large induced current demand during power-down

Intelligent Distributed Architecture

Access may be restricted based on Time of Day, Day of Week, and Door. Access may be granted when the user presents the correct code, card, or both. The user may be granted temporary access based on Use Count Limits, Temporary Day Limits, and Absentee Rule Limits, with Auto-Disable or Auto-Delete on Expiration of Temporary Users. Additional functions include Unlock/Relock, Alarm Mask/Unmask, and Lock Down/Lock Down Release. The associated door may be monitored for Door Forced Open and Door Open Too Long, while providing Auto Relock Control.

High Security Alarm Monitoring

Identity uses very stable digitally processed analog inputs with line supervision for high-security alarm monitoring. A line supervision module is located at the door contact, alarm sensor, request to exit (RQE), or similar device to establish this supervision. Conditions reported include Alarm, Secure, Short, Open, Noisy, and Input-Out-of-Spec.

Reliability by Design

Mx1 Controllers are designed for high availability as a complete system for global markets. A standby battery for memory is standard, while a standby UPS or battery for operation is optional. The controller ships ready to be connected to a PoE+ power source, and has support for optional external power supplies. Power connectors are fused. Readers and relays are protected by built-in hardware circuits which will cut off power when they detect over-power consumption, protecting the board against unintended damage.

Features and Benefits

The Mx1 has a built-in Secure Network Interface Board 3 (SNIB3) with enhanced memory storage at 500K credentials, security, TLS, 128-bit, or 256-bit encryption options, and network functionality and capabilities. The SNIB3 is a leading edge communication device that provides IPv6, Gigabit Ethernet, and IEEE 802.3 certified cryptography, including AES 256.

hirschsecure.com • sales@hirschsecure.com • +1 888-809-8880
Hirsch is part of the Vigilant Group.

HIRSCH DATA SHEET
Title Title Title
Subtitle subtitle subtitle

Cirrus Network Installation Diagram

Contact Information

Optimize your Identity product implementation and support efforts with professional project management. Ensure efficiency, reduce risks, and maintain high-quality support services to achieve successful product deployments.

For inquiries, pricing, and technical support, please contact us at:

HIRSCH
TECHNICAL DATA IS SUBJECT TO CHANGE WITHOUT NOTICE. REVISION DATE: 2023-07-15
© Hirsch, Inc. All rights reserved. This document is Hirsch public information.