Cybersecurity Policy Overview

A. Purpose:

This document is intended to provide an overview and summary of Chroma Software, Inc.'s ("Chroma") Cybersecurity Policy, including the scope, ownership, and structure of the policies in place at Chroma, as well as the topic areas and industry standards addressed by the Cybersecurity Policy.

B. Audience and Availability:

The policy overview is intended for any external parties (potential clients, auditors, regulators, etc.) who wish to understand how Chroma addresses service requirements and industry best practices through its framework of cybersecurity policies. Any further distribution of this document beyond the intended recipient(s) must be approved by Chroma.

Chroma policies are made available to all workforce members via shared network resources. Through periodic security and training updates, and new hire training, all Chroma workforce members are made aware of how to access Chroma policies.

C. Ownership:

This overview is owned and maintained by the Chroma Chief Technology Office ("CTO"). Please contact the identified owner(s) for questions or additional information.

D. Cybersecurity Policies Overview:

Chroma's Cybersecurity Policy has a defined scope outlined at the beginning of the document in the "**Scope**" section, generally intended to apply to Chroma workforce members, including full-time employees, part-time employees, contractors, consultants, and others as applicable.

The ownership of the Cybersecurity Policy is defined in the **"Ownership"** section. The document owner is responsible for maintenance and review of the policy to ensure it is an accurate and up-to-date reflection of policies, procedures, and corresponding operational practices at Chroma. The owner is also a point of contact for any questions or additional information which the audience of the policy and/or procedures may have.

In certain circumstances, exceptions to the policy statements within Chroma's Cybersecurity Policy will be permitted with approval from the CTO, or designee. The "**Exceptions**" section of our Cybersecurity Policy details how these may be requested. Similarly, violations of the policies and procedures shall be dealt with in accordance with Chroma disciplinary policies and/or procedures, and the Cybersecurity Policy has an "**Enforcement**" section to address this.

The policy content is then set out in the "**Policy"** sections of the Cybersecurity Policy, subsequently.

Also included is a "**Revision History**" section with details of what action was taken to create, update or review the document, what date this action occurred, and any other applicable notes, such as approver and version controls.

A documented mapping of the NIST Cybersecurity Framework to Chroma's ensures that the policies in place at Chroma are effective in meeting the required topic areas and industry standards.

E. Policies Summary:

General Cybersecurity-related Policy Topic Areas:

The below topic areas are governed by Chroma's Cybersecurity Policy, with the objective of protecting the security, confidentiality, integrity, availability, and privacy of information within the Chroma information ecosystem, at all stages of the information lifecycle. Topic coverage of Chroma policies and procedures includes, without limitation:

- Asset Management: policies are in place providing the overall framework for the management of devices capable of storing or processing Chroma information. Controls are defined to ensure that all IT assets are used in a safe and consistent manner to maximize the security of sensitive information and to optimize the use of all IT assets throughout the organization.
- Acceptable Use: workforce members are required to acknowledge and comply with acceptable usage of Chroma assets and information. Workforce members are responsible for ensuring the security and appropriate use of Chroma's assets and information and protecting these against unauthorized use, damage, or loss.
- Security Roles and Responsibilities: policies are in place to outline the roles and responsibilities of Chroma's Security Officer and workforce members, with respect to the execution of Chroma's information security program.
- Security Governance and Risk Management: policies are in place to ensure that Chroma has designated personnel and programs in place to govern privacy and security programs and adhere to compliance obligations, including the development of robust internal policies, periodic risk assessments and security assessments to identify potential internal and external vulnerabilities, and subsequently taking action to remediate vulnerabilities.
- Third-Party Risk Management: policies are in place governing the security, privacy, compliance, and general risk requirements for engaging third parties, including: assessment of third parties prior to and during their engagement to identify and mitigate risk, third-party obligations, and supervision of third parties.
- Access Control: policies are in place defining the security requirements for establishing system accounts, controlling access to applications or systems, and ensuring that users are authorized to access Chroma information. Controls are also in place to ensure that periodic access reviews are performed, that the principles of segregation of duties are enforced, that access to information is granted and revoked in a timely manner and with relevant approvals (and based on user need to access information in Chroma systems and facilities), and that strong passwords are enforced.
- Remote Access: polices are in place to ensure that Chroma implements the proper security measures for the remote workforce including multi-factor authentication.
- Security Awareness and Training: Chroma ensures that the workforce is trained upon hiring, and periodically, with regard to information security best practices appropriate for the workforce's job roles and responsibilities.
- Data Security: Chroma exercises its responsibility to protect data in its custody with industry standard protection mechanisms including, but not limited to, encryption, segregation of environments, and endpoint protection.
- Data Backup: Chroma ensures the continuity of its operations through the use of secure, repeatable, and automated back-up processes that are regularly tested.
- Vulnerability Management: policies are in place to reduce the risk and exposure posed by technical vulnerabilities in Chroma assets and information. Chroma performs periodic vulnerability scans to identify potential internal and external vulnerabilities, and subsequently takes action to remediate identified vulnerabilities.

- Configuration Management: policies are in place to ensure the establishment of baseline configurations for Chroma information assets, employing the principle of least functionality.
- Change Management: policies are in place ensuring that Chroma implements mechanisms for securely requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. Controls are defined to ensure that all changes are properly documented, approved, tested, and scheduled prior to implementation.
- Physical Security: policies and procedures are in place governing the physical safety and security requirements for Chroma information assets, ensuring Chroma assets and information are protected from unauthorized access, theft, or tampering.
- Business Continuity: policies and procedures (including Business Continuity Plans) are in place serving to ensure that the information systems and business processes that provide critical functionality for Chroma business are predefined and the procedures that guide immediate response and subsequent recovery of these systems and processes are documented to help ensure availability and continuity. Chroma requires that recovery team members be adequately trained in recovery procedures and the restoration of critical business systems in the event of planned or unplanned events.
- Audit: policies are in place ensuring that Chroma implements mechanisms to record and examine activity in information systems to ensure it has not been accessed, altered, or destroyed in an unauthorized manner. Controls are defined to govern the logging and monitoring of activities in Chroma systems at the network, application, and database levels, and enabled to monitor discrepancies and provide historical perspective for auditing and required reporting.
- Network Security: Chroma ensures that any network that its data resides on or is transferred through is protected and configured in accordance with industry best practices.
- Cloud Security: The cloud security policy extends the requirements set forth by existing information security policies to the cloud environments it uses.
- Incident and Breach Response: policies and procedures (including Incident Response Plans) are in place establishing the coordination of Chroma response to any security or privacy incident. Chroma has established lines of communication which enable the timely reporting of possible incidents to Chroma's Incident Response Team. The Incident Response team has been trained, and performs annual exercises, on the performance of assessments of possible incidents, to identify potential risks and impacts to both Chroma and its customers. Chroma has defined the necessary actions for incident response with respect to documentation, investigation, and remediation of incidents.