BLUE ROSE

Blue Rose Consulting Group Inc

Data Security & Privacy Policy

Table of Contents

1. PURPOSE **3**

2. SCOPE **3**

3. ROLES & RESPONSIBILITIES **3**

3.1 All Team Members 3

3.2 Managers & Project Leads 3

3.3 Operations & Compliance 3

4. POLICY STATEMENTS **3**

4.1 Confidential Information Safeguards 3

4.2 Personal Data Handling 3

4.3 Use of Company IT Systems 4

4.4 Unauthorized Access Prohibited 4

4.5 Media & Recording Restrictions 4

4.6 Physical & Government-Classified Security 4

4.7 HR & Medical Records 4

4.8 Responsible Use of Emerging Technology 4

5. SMS PRIVACY NOTICE **5**

6. PRACTICAL GUIDELINES **5**

7. INCIDENT REPORTING & ESCALATION **5**

8. RELATED POLICIES & REFERENCES **6**

REVISION HISTORY

Version	Date	Updates	Authorized By
V1.0	01/06/2022	▪ Initial issue aligning handbook with 2025 Privacy Policy	Operations & Compliance
V2.0	2/06/2025	▪ Annual Review	David M. Savage
V3.0	2/06/2026	▪ SMS Privacy Statement Added	David M. Savage

1. Purpose

Blue Rose Consulting Group ("Blue Rose") is committed to protecting the confidentiality, integrity, and availability of Company, client, and employee information. This section outlines the rules that safeguard data and preserve privacy across our operations.

2. Scope

This policy applies to all employees, contractors, temporary staff, interns, and third-party service providers who create, access, store, transmit, or process information on behalf of Blue Rose.

3. Roles & Responsibilities

3.1 All Team Members

- Protect non-public information and only access it when required for legitimate business purposes.
- Immediately report suspected data breaches or privacy incidents.

3.2 Managers & Project Leads

- Enforce this policy within their teams and ensure adequate access controls.
- Review and approve any data-sharing with external parties.

3.3 Operations & Compliance

- Maintain this policy, conduct training, and perform periodic audits.

4. Policy Statements

4.1 Confidential Information Safeguards

All non-public Company, client, and partner information is proprietary and must be stored in approved, access-controlled repositories and shared on a need-to-know basis.

4.2 Personal Data Handling

Personal information must be collected, processed, and retained only for lawful, disclosed purposes, with appropriate administrative, technical, and physical safeguards in place.

4.3 Use of Company IT Systems

Email, instant messaging, and other IT systems are Company property. Blue Rose may monitor, access, or disclose content to protect its interests; therefore, users should not expect privacy on these systems.

4.4 Unauthorized Access Prohibited

Attempting to access another individual's files, messages, or accounts without explicit permission is strictly prohibited and may result in disciplinary action.

4.5 Media & Recording Restrictions

During working time, employees may not photograph, film, or record work areas, client documents, or government-related materials to prevent accidental data exposure.

4.6 Physical & Government-Classified Security

When work involves government classified contracts or controlled information, Blue Rose will implement any additional physical or procedural controls required by contract or law.

4.7 HR & Medical Records

Personnel and medical records are maintained in secure, separate repositories and are accessible only to authorized HR staff on a need-to-know basis.

4.8 Responsible Use of Emerging Technology

Artificial intelligence and similar tools may be used only when they are ethical, transparent, privacy compliant, and subject to human oversight for critical decisions.

5. SMS Privacy Notice

Blue Rose Consulting may collect your mobile phone number when you opt in to receive SMS messages from us, including when you provide verbal consent during a phone call or in person with a representative. Verbal consent is documented before any SMS messages are sent. Mobile information will not be shared with third parties or affiliates for marketing or promotional purposes. All categories exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties.

If you opt in, you may receive SMS messages related to customer care, account notifications, service updates, scheduling, billing communications, or other business-related messaging. Message frequency may vary. Message and data rates may apply.

You may opt out at any time by replying STOP. For help, reply HELP or contact us at:

Website: Home - Blue Rose Consulting Phone: 202-774-2059

6. Practical Guidelines

Label and secure any document containing personal or client data.

Use Blue Rose-approved communication channels; never route business through personal accounts.

Think before sharing—if information is not intended for the public domain, keep it off social media, public calls, and screenshots.

Protect laptops and mobile devices with strong authentication and encryption.

7. Incident Reporting & Escalation

Report any suspected data breach, loss, or unauthorized disclosure immediately to Operations at **operations@bluerose-consulting.com** or via our main company line (**202-774-2059**). The Compliance team will coordinate containment, investigation, and regulatory notifications.

8. Related Policies & References

- Code of Ethics & Business Conduct
- Acceptable Use of Information Systems
- System Security Plan (SSP)Version 2.1
- Blue Rose Consulting Group Inc - Incident_Response_Policy