



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

LETTER OF AUTHORIZATION / NON-DISCLOSURE AGREEMENT (NDA)

To,
The Cyber Expert & Cyber Forensic Analyst
Cyber Privilege

Place: _____

Date : _____

Send scanned, duly signed file with all supporting documents to:

✉ investigate@cyberprivilege.com

Subject: Request for Private Assistance and Investigation support in FIR No: _____

U/Sec _____ IT Act, U/Sec _____ IPC, P.S. _____, City, District,
State _____ NCR/Cybercrime Acknowledgment

No: _____ Dated _____.

Application under Criminal Procedure Code (Cr.PC) Section 457 for release/refund of frozen funds in bank account.

Respected Sir,

I, the undersigned, hereby authorize Cyber Privilege, represented by its Cyber Expert & Cyber Forensic Analyst, to extend professional assistance in connection with the above-mentioned case. This includes but is not limited to:

- Coordinating with the Investigating Officer with LEA if Required.
- Providing and certifying relevant electronic/digital evidence.
- Allowing examination of mobile phone(s), devices, or digital assets if required.
- Assisting with legal proceedings including filing before the Chief Metropolitan Magistrate Court as Annexure-II in the victim's petition.
- Liaising with financial institutions, banks, NBFCs, and other authorities to facilitate release/refund of frozen funds. Handling complaints relating to cybercrimes involving SB/CA bank accounts, credit cards, debit cards, digital wallets, or other financial/electronic evidence.

I understand and acknowledge that:

1. Charges incurred are strictly non-refundable.
2. Cyber Privilege acts only as an assisting/forensic expert and does not guarantee any particular outcome.
3. Any liabilities arising are subject to applicable cyber insurance policies, not Cyber Privilege.
4. All cooperation from my side is mandatory. In the event of withdrawal, non-cooperation, or suppression of facts, Cyber Privilege reserves the right to close the case without liability. Any complaints related to cybercrime must be directed to the appropriate law enforcement/cybercrime authority, and Cyber Privilege will extend assistance accordingly.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

LETTER OF AUTHORIZATION / NON-DISCLOSURE AGREEMENT (NDA)

Verification & Affirmation

I, _____ (S/o / D/o _____), holder of Aadhaar No. _____, do hereby solemnly affirm and declare that:

- All facts, documents, and screenshots submitted by me are true, correct, and complete to the best of my knowledge and belief.
- No material fact has been concealed or misrepresented.
- I fully understand and agree that there are no warranties or assurances regarding the completion of the process.
- I have submitted my KYC details for verification and undertake to provide any further documents/evidence required.
- I hereby sign and execute this Letter of Authorization / Non-Disclosure Agreement voluntarily and unconditionally, with full consent.

Thanking you,

Yours faithfully,

(Signature of Deponent)

Name: _____

Contact No: _____

Email ID: _____

Mandatory Requirement:

This document must be digitally signed via DigiLocker and emailed to investigate@cyberprivilege.com along with all supporting details.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

PUBLIC NOTICE, TERMS OF ENGAGEMENT, RULES & REGULATIONS, AND PRIVACY POLICY

PUBLIC NOTICE, TERMS OF ENGAGEMENT, RULES & REGULATIONS, AND PRIVACY POLICY

Issued by Cyber Privilege Dt: 01/02/2024

This Public Notice constitutes a formal declaration of Cyber Privilege's binding Terms of Engagement, Privacy Policy, Rules & Regulations, and Legal Liabilities applicable to all clients, consumers, collaborators, associates, interns, and members of the general public who engage with Cyber Privilege in any capacity. By accessing our platforms, contacting our team, or availing our services, you irrevocably consent to these Terms and Conditions.

1. Scope of Services & Best-Effort Disclaimer

Cyber Privilege delivers specialized, high-level professional services including but not limited to:

- Cyber Security Services – vulnerability assessment, penetration testing, SOC monitoring.
- Cyber Forensics – recovery and analysis of digital evidence, device imaging, WhatsApp forensics, RAT investigations.
- Digital Clue Identification & Evidence Collection – collection, preservation, and authentication of digital artifacts.
- Legal Liaison Support – drafting emails, escalation documents, and assisting with law enforcement reporting.
- Electronic Evidence Certification – issuance of certificates under Section 65B of the Indian Evidence Act or Section 63(4)(C) Part-B, ensuring evidentiary admissibility in courts of law.

Important Disclaimer:

All services are delivered strictly on a best-effort basis and are subject to:

- No Warranty
- No Guarantee
- No Refund
- No Return of Payments

Cyber Privilege assumes no liability for financial outcomes, litigation results, or external law enforcement actions beyond the scope of contracted deliverables.

2. Legal Standing & Binding Framework

- All communications, clarifications, cost structures, and processes are issued strictly without prejudice.
- Nothing herein shall be treated as a waiver, admission, or binding contract unless executed under a duly signed Service Agreement.
- Annexure I-XXXVIII of Cyber Privilege's internal policies form an integral part of all engagements.
- Cyber Privilege ensures compliance with:
 - General Data Protection Regulation (GDPR)
 - Digital Personal Data Protection Act, 2023 (DPDP Act)
 - ISO/IEC 27001:2013 Information Security Protocols
 - CIA Triad Security Framework (Confidentiality, Integrity, Availability)

All liabilities in litigation, financial disputes, and law enforcement proceedings remain the sole responsibility of the client.

3. Rules of Engagement

All clients, associates, and third parties must strictly adhere to the following engagement protocols:

- All communications must remain respectful, lawful, and professional.
- Any form of scolding, harassment, threats, abusive language, intimidation, defamatory remarks, or spreading false allegations against Cyber Privilege or its stakeholders is strictly prohibited.
- This protection extends to all persons connected with Cyber Privilege, including but not limited to:
 - CEO, CTO, COO, and Directors
 - HR Managers and Coordinators
 - Alpha Team Members, Hackers, Analysts, and Investigators
 - Interns, Associates, Volunteers, and Advisors



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

PUBLIC NOTICE, TERMS OF ENGAGEMENT, RULES & REGULATIONS, AND PRIVACY POLICY

4. Legal Consequences of Misconduct

Cyber Privilege maintains zero tolerance for misconduct.

Any violation of the above rules shall attract severe legal consequences, including but not limited to:

- Civil Penalties ranging from ₹5 Crores to ₹50 Crores.
- Defamation Lawsuits under IPC Sections 499 & 500 and provisions of the Information Technology Act, 2000, carrying damages of ₹5 Crores to ₹50 Crores.
- Criminal Proceedings with potential imprisonment of up to 7 years.
- Permanent Blacklisting from all Cyber Privilege services and networks.
- Escalation to Law Enforcement Agencies (LEA), National Cybercrime Reporting Portal, and relevant judicial authorities.

 **Be Warned:** Defamation or harassment of Cyber Privilege or its members is not merely a contractual violation but a criminal act that will be pursued to the maximum extent of law.

5. Privacy & Confidentiality

Cyber Privilege enforces uncompromising data protection and confidentiality measures, including:

- GDPR Compliance – adherence to international data handling standards.
- DPDP Act 2023 – strict compliance with Indian data protection laws.
- ISO/IEC 27001:2013 – certified information security management practices.
- CIA Triad Framework – ensuring Confidentiality, Integrity, and Availability of all digital evidence.
- Confidentiality Annexures (I-XXXVIII) – specialized internal protocols for sensitive data, victim assistance, and case management.

 All communications are logged, timestamped, encrypted, and monitored for compliance and evidentiary admissibility. Unauthorized access, duplication, or misuse is strictly prohibited and will trigger immediate prosecution.

6. Special Policies for Clients & Victims

- All evidence submissions must follow official Cyber Privilege channels.
- Circumvention, informal sharing, or unauthorized disclosure of evidence is invalid and unlawful.
- Victims of cybercrime are granted special protections, including strict confidentiality and restricted access handling under Victim Protection Guidelines.
- Cyber Privilege reserves the right to decline service where compliance, legality, or safety is compromised.

7. Final Warning & Irrevocable Consent

By engaging with Cyber Privilege — whether through calls, emails, WhatsApp, evidence portals, or personal meetings — you automatically consent to the above:


- Terms & Conditions
- Privacy Policies
- Confidentiality Rules
- Penalties for misconduct

 Any breach of these terms will be treated as willful misconduct and prosecuted with the strictest financial, civil, and criminal penalties under applicable law.

8. Contact & Reporting

For all lawful communications, queries, or escalations, contact only through official channels:

 investigate@cyberprivilege.com

 case@cyberprivilege.com

 www.cyberprivilege.com

Cyber Privilege

Saviors of Truth | Peace Finders | Digital Guardians



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

Terms & Conditions – Cyber Privilege

Jurisdiction: Vijayawada, Andhra Pradesh, India & Hyderabad, Telangana, India (PAN-India & International Applicability) Effective Date: 01/02/2024

Cyber Privilege (“Cyber Privilege”) is a globally recognized Cybersecurity and Cyber Forensics Organization, engaged in the lawful business of cyber forensics, evidence certification, darknet research, cybercrime investigations, cybersecurity assessments, and allied services.

These Terms & Conditions (hereinafter referred to as “Agreement”) shall govern all interactions, enquiries, communications, service engagements, contracts, calls, consultations, forensic assignments, training programs, internships, research programs, and all professional dealings with Cyber Privilege.

By visiting our website, contacting our official helpline (+91-8977308555), emailing us, engaging our services, or entering into any communication, you (“the Client/User/Enquirer/Party”) hereby expressly agree to be bound by the terms of this Agreement.

1. Scope of Agreement

1.1 These Terms govern all communications, proposals, enquiries, calls, cost structures, forensic certifications, analyses, training, research, internships, volunteer engagements, cyber investigations, and legal support undertaken by Cyber Privilege.

1.2 No oral conversation, enquiry, WhatsApp message, email, consultation, or preliminary communication shall be construed as a binding contract or commitment.

1.3 A service engagement shall be legally binding only upon execution of a written Service Agreement, duly signed and sealed by the authorized representatives of Cyber Privilege.

2. Without Prejudice & Non-Waiver

2.1 All reports, certifications, clarifications, proposals, and cost quotations are issued strictly without prejudice.

2.2 Nothing said, written, or communicated by Cyber Privilege, its Board of Directors, CEO, CTO, Senior Management, Human Resource, Legal Team, Accounts Team, Employees, Associates, Interns, or Volunteers shall:

- Constitute an admission of liability; Be interpreted as a waiver of rights; Form a binding contractual obligation; Create enforceability in any court of law,

...unless expressly incorporated into a duly signed and executed Service Agreement.

3. Prohibited Hostile Enquiries, Manipulations & Honey Traps

3.1 Any enquiry, call, email, or communication made with malicious intent, hostile questioning, manipulation, inducement, deception, emotional exploitation, honey trapping, or entrapment tactics is strictly prohibited and deemed unlawful.

3.2 The following acts shall be treated as grave breaches of contract and malicious misconduct:

- Fake victim calls designed to deceive Cyber Privilege staff.
- Pretended women/female clients claiming victimhood to emotionally manipulate Cyber Privilege representatives.
- Attempts to create false intimacy, sexual innuendos, personal conversations, harassment, or emotional entrapment.
- Recording calls or communications without lawful sanction and maliciously presenting them before Law Enforcement Agencies (LEA), media, or courts to defame, intimidate, or harass Cyber Privilege.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

Terms & Conditions – Cyber Privilege

3.3 Penalty Clause:

- Any person(s), entity, client, or agency engaging in such prohibited actions shall be liable to a monetary penalty of not less than ₹5 Crores (Fifty Million INR) and up to ₹50 Crores (Five Hundred Million INR), enforceable through civil proceedings, arbitral awards, and criminal prosecutions under Indian laws, including but not limited to the Indian Penal Code (IPC), Information Technology Act, Bharatiya Sakshya Adhiniyam (BSA) 2023, and allied legislations.

3.4 Cyber Privilege reserves the right to initiate:

- Civil suits for damages in competent courts;
- Criminal complaints and FIRs against offenders;
- Permanent blacklisting of individuals/entities engaging in such misconduct;
- Publication of offending conduct for public awareness and deterrence.

4. Client Responsibility & Liability

4.1 The Client/User/Enquirer assumes exclusive liability for all actions, representations, and consequences arising out of engagement with Cyber Privilege.

4.2 Cyber Privilege shall not be held responsible for:

- Misuse, alteration, falsification, or misrepresentation of reports.
- Adverse legal outcomes in court, arbitration, regulatory, or police proceedings.
- False claims, fabricated evidence, or hostile allegations intended to exploit or defame Cyber Privilege.

5. Cyber Forensics, Darknet & Research Engagements

5.1 Cyber Privilege conducts darknet monitoring, OSINT, SOCMINT, digital profiling, malware forensics, and cyber investigations strictly for lawful and ethical purposes.

5.2 Clients acknowledge that misuse of any forensic report, certification, research, or intelligence for illegal activities, harassment, or defamatory purposes shall attract full liability against the Client.

6. Limitation of Liability

6.1 Cyber Privilege, including its Board, CEO, CTO, Directors, Legal, Accounts, Human Resources, Employees, Interns, Associates, and Volunteers, shall not be liable for:

- Any direct, indirect, incidental, or consequential damages.
- Emotional distress, defamation, reputational harm, or financial losses suffered by the Client.

6.2 The maximum liability of Cyber Privilege under any service agreement shall be strictly limited to the total professional fee paid by the Client for that specific service engagement.

7. Data Privacy & Compliance

7.1 Cyber Privilege complies with:

- GDPR (European Union),
- Digital Personal Data Protection Act, 2023 (India),
- CIA Triad Standards (Confidentiality, Integrity, Availability).

7.2 Clients expressly consent to Cyber Privilege's lawful right to:

- Process, preserve, encrypt, or store data,
- Retain digital evidence for audit/legal requirements,
- Submit evidence to courts or authorities only under lawful compulsion.

8. Interns, Volunteers & Associates

8.1 Interns, researchers, trainees, and volunteers operate under strict NDAs and ethical codes.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

Terms & Conditions – Cyber Privilege

8. Interns, Volunteers & Associates

8.1 Interns, researchers, trainees, and volunteers operate under strict NDAs and ethical codes.

8.2 They are not authorized to bind Cyber Privilege into any contractual or legal obligation.

8.3 Unauthorized statements or actions by interns, volunteers, or associates shall be deemed void and unenforceable.

9. Intellectual Property Rights

9.1 All research methodologies, forensic tools, spectrograms, waveforms, annexure templates, certifications, training modules, investigative frameworks, and proprietary technologies are the exclusive property of Cyber Privilege.

9.2 Clients are granted a limited, case-specific, non-transferable license solely for lawful use of reports and certifications. Redistribution, resale, disclosure, or misuse of Cyber Privilege's IP shall constitute intellectual property infringement and invite prosecution.

10. Indemnification

The Client/User/Enquirer hereby covenants to indemnify, defend, and hold harmless Cyber Privilege, its officers, directors, human resources, employees, interns, volunteers, and associates from any and all claims, liabilities, damages, penalties, expenses, or proceedings (including attorney's fees) arising from:

- Hostile or manipulative enquiries,
- Honey traps, false allegations, or fabricated evidence,
- Misuse or unauthorized disclosure of forensic deliverables.

11. Jurisdiction & Governing Law

11.1 This Agreement shall be governed by the laws of India.

11.2 The exclusive jurisdiction for all disputes shall rest with the competent civil and criminal courts of Vijayawada, Andhra Pradesh, and Hyderabad, Telangana.

11.3 International Clients submit irrevocably to the jurisdiction of Indian Courts.

12. Termination of Services

12.1 Cyber Privilege reserves the unilateral right to deny, suspend, or terminate services at any stage if:

- The Client fails to make payment,
- The Client engages in hostile, unethical, or unlawful behavior,
- The Client attempts entrapment, harassment, or emotional exploitation.

12.2 No refunds shall be made upon such termination unless explicitly provided under a separate written agreement.

13. Force Majeure

Cyber Privilege shall not be liable for failure or delay in performance of obligations where such failure arises due to circumstances beyond reasonable control, including but not limited to:

- Natural disasters, pandemics, strikes, riots,
- Cyberattacks, governmental restrictions, or political unrest.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

Terms & Conditions – Cyber Privilege

14. Amendments

Cyber Privilege reserves the right to amend, modify, or update these Terms & Conditions without prior notice. All updates shall be binding upon publication on www.cyberprivilege.com.

📌 Key Protective Clauses

👉 Cyber Privilege, its Board, CEO, CTO, Legal, Accounts, HR, Employees, Interns, Associates, and Volunteers shall not, under any circumstances, be personally or collectively liable for hostile enquiries, manipulations, false victim claims, honey traps, or fabricated evidence.

👉 Any such malicious act shall automatically invoke penalties of ₹5 Crores – ₹50 Crores, alongside civil recovery, criminal prosecution, FIRs, and blacklisting of the offending individual/entity.

👉 All risks, liabilities, and consequences rest solely and exclusively with the Client/User/Enquirer.

I have sought assistance from Cyber Privilege represented by their Cyber Expert & Cyber Forensic Analyst, to collaborate with law enforcement agencies, as well as financial institutions including bankers and NBFCs. They will handle cases involving complaints regarding cyber crimes related to SB/CA Bank Accounts, Credit Cards, Debit Cards, and any other pertinent evidence. I acknowledge that the charges incurred are non-refundable. Any parties with complaints about cyber crimes should be directed accordingly.

Statutory Warning: Attempting to call sms WhatsApp to 8977308555 📞📧 sms/WhatsApp or call 📞 us more than twice will result in immediate blocking. Further consequences will be enforced without delay

Online Consent Letter Terms and Conditions, Privacy Policy, Secure Confidential trust principles of Confidentiality, Integrity & Availability (CIA Triad), Legal Disclaimer & Proper Verification :

I, _____ S/o. _____ D/o.. _____ Aadhaar Number: _____
Address: _____

_____ the deponent, do hereby solemnly affirm and declare that the contents and screenshots of the conversation provided herein are true to the best of my knowledge and belief. I affirm that no material facts have been withheld, and there is no falsehood contained in any part of this affidavit. I acknowledge that there are no assurances or guarantees regarding the completion of this task, and any liabilities shall be subject to the terms of relevant cyber insurance policies rather than Cyber Privilege. I fully comprehend and have signed the Letter of Authorization/Non-Disclosure Agreement. I have provided all necessary details, including KYC, for verification purposes, and I commit to cooperating with the investigation team unconditionally. I understand that failure or cessation of cooperation at any stage may result in the closure of the case from my end.

Thanking you sir,

Yours Obediently,

NDA Should Digilocker signed and send to us



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

🚫 No Refund & No Return Policy – Cyber Privilege

Effective Date: 01/02/2024

Jurisdiction: Vijayawada, Andhra Pradesh & Hyderabad, Telangana (PAN-India & International Enforcement)

Cyber Privilege ("we", "our", "us") operates under a strict No Refund and No Return Policy. By engaging with our services, accessing our digital platforms, or making any financial transactions with us, you ("Client", "Customer", "User", or "Party") hereby irrevocably agree and accept the following terms:

1. Absolute No Refund Policy

1.1 All fees, charges, retainers, and payments made to Cyber Privilege for forensic, investigative, cybersecurity, compliance, training, consultancy, digital evidence, or any associated services are non-refundable under any circumstances.

1.2 Once payment is initiated, processed, or received (in whole or in part), the Client forfeits any and all rights to claim, demand, dispute, or enforce refunds.

1.3 This clause remains binding even if:

- Services are delayed.
- Work is ongoing, incomplete, or in progress.
- Work is partially done or not delivered due to force majeure.
- The Client changes their mind, disengages, or withdraws cooperation.

2. Absolute No Return Policy

2.1 Cyber Privilege does not accept returns of goods, digital reports, certifications, software, or any deliverables.

2.2 Forensic reports, certifications, data analysis, evidence files, training modules, digital handbooks, or consultancy outputs once delivered (physically, digitally, or verbally) are considered final and non-returnable.

2.3 Clients, customers, or entities shall have no right to demand replacements, alternate versions, or re-issuance of reports or services, except under a new and separate contract.

3. No Right to Question or Delay Disputes

3.1 The Client hereby expressly waives the right to question, dispute, or interrogate Cyber Privilege regarding:

- The timeline or process of service delivery.
- The internal methodologies, research, or techniques used.
- Delays caused due to law enforcement liaison, court procedures, or evidence handling.

3.2 Any attempt by the Client to harass, intimidate, or force explanations shall be deemed a hostile act and may attract penalties of ₹5 Crores – ₹50 Crores, along with civil and criminal proceedings.

4. Binding Nature of Engagement

4.1 All engagements are final, non-reversible, and binding upon payment or execution of a Service Agreement.

4.2 The Client acknowledges that digital forensic, cybersecurity, and investigative services are professional expertise-based engagements that cannot be undone, reversed, or retracted once commenced.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

4.2 The Client acknowledges that digital forensic, cybersecurity, and investigative services are professional expertise-based engagements that cannot be undone, reversed, or retracted once commenced.

4.3 Any dispute shall not invalidate this No Refund, No Return Policy.

5. Client Responsibility

5.1 The Client bears sole responsibility for:

- Ensuring correct submissions, instructions, or evidence provided to Cyber Privilege.
- Verifying their intent before engaging services.
- Understanding the non-refundable, non-returnable nature of the engagement.

5.2 Cyber Privilege shall not be liable for misunderstandings, assumptions, or lack of due diligence on the part of the Client.

6. Exceptions – None

6.1 No exceptions exist under this policy.

6.2 Refunds and returns are strictly prohibited even in the following cases:

- Dissatisfaction with service.
- Non-acceptance of findings.
- Failure of evidence to support client's legal position.
- Internal client disputes or third-party pressures.

7. Force Majeure

7.1 In case of delays or non-performance due to natural disasters, cyberattacks, pandemics, governmental orders, court restrictions, or technical failures, Cyber Privilege remains fully indemnified.

7.2 Such events shall not constitute grounds for refunds, returns, or cancellation.

8. Legal Enforcement

8.1 This No Refund & No Return Policy forms part of the Terms & Conditions and Service Agreements of Cyber Privilege.

8.2 Clients expressly waive the right to raise consumer claims or financial disputes under general refund laws, as Cyber Privilege operates under specialized forensic, investigative, and cybersecurity service exemptions.

8.3 All disputes shall fall exclusively within the jurisdiction of Vijayawada, Andhra Pradesh & Hyderabad, Telangana Courts.



CYBER PRIVILEGE

Cyber Expert
&
Cyber Forensic
Services

EVIDENCE



CYBER PRIVILEGE

An ISO 9001:2015 Certified Organization

#Hyderabad, Branch: Vijayawada

EMAIL :- investigate@cyberprivilege.com

EMAIL :- case@cyberprivilege.com

Digital Evidence Collection and Certification with Hash Values: MD5, SHA1, SHA256, SHA512

Key Protective Clauses

- All payments are final, binding, and non-recoverable.
- Clients have no legal right to demand refunds, returns, or questioning of processes.
- Hostile enquiries or refund/return demands may invite financial penalties (₹5 Crores – ₹50 Crores), civil recovery suits, and criminal proceedings.
- Cyber Privilege, its Board, CEO, CTO, Legal, Accounts, Employees, Interns, Volunteers, and Associates remain fully protected, indemnified, and shielded under this policy.

Acknowledgement of Client/Party 100% Consent towards Cyber Privilege :

By engaging with Cyber Privilege, the Client expressly confirms:

- ✓ I understand and accept that all payments are non-refundable.
- ✓ I waive all rights to returns, replacements, or refunds.
- ✓ I waive the right to question delays, processes, or internal methodologies.
- ✓ I accept full liability for my engagement and absolve Cyber Privilege of financial responsibility.

Client/Authorized Signatory:

Name: _____

For Cyber Privilege (Authorized Representative):

Name: _____

Signature: _____

Date: _____

Signature : _____

Designation: _____

Witness 1: Name: _____ Signature: _____ Date: _____

Witness 2: Name: _____ Signature: _____ Date: _____