



AIH Hub For Cloud Service & Datacenters Providers L.L.C

OFFICIAL COMPANY POLICY

Professional Conduct & De-escalation Standard (PCDS)

Policy, Compliance Annex, Agent SOP, and Ticket Template Pack

Effective Date: 21 April 2026

Document Number: PCDS-001

© 2026 AIH Hub For Cloud Service & Datacenters Providers L.L.C . All rights reserved.

AIH Hub For Cloud Service & Datacenters Providers L.L.C .

522B, Standard Chartered Tower Burj Khalifa, Dubai, UAE

Phone +971-4313-2565 Website: www.aihostinghub.ae

Trademarks

AIH PCDS Official Company Policy | PCDS-001 are registered trademarks of AIH. All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. AIH disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall AIH be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if AIH or its suppliers have been advised of the possibility of such damages.

Document Lifetime

AIH may occasionally update online documentation between releases of the related software. Consequently, if this document was not downloaded recently, it may not contain the most up-to-date information. Please refer to www.aihostinghub.ae/PCDS for the most current information.

From the Web site, you may also download and refresh this document if it has been updated, as indicated by a change in this date: June 10, 2026

Where to get help

AIH support, product, and licensing information can be obtained as follows.

Product information — Documentation, release notes, software updates, and information about AIH products, licensing, and service, are at AIH Support website at:

<https://support.aihostinghub.ae>

Technical support — Go to <https://support.aihostinghub.ae> . On the Support page, you will see several options, including one for making a service request. Note that to open a service request, you must have a valid support agreement.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please submit your opinion of this document to:

<https://support.aihostinghub.ae>

If you have issues, comments, or questions about specific information or procedures, please include the title and, if available, the part number, serial number, the revision, the page numbers, and any other details that will help us locate the subject that you are addressing.

Table of Contents

Document Control.....	5
Approval and Sign-Off	5
Professional Conduct & De-escalation Standard (PCDS) Policy	5
1. Purpose	5
2. Scope	5
3. Policy Statement	6
4. Guiding Principles	6
5. Definitions	6
6. Standards of Acceptable Conduct	6
7. Prohibited Conduct.....	7
8. De-escalation Protocol	7
9. Enforcement Levels	7
10. Zero-Tolerance Categories.....	7
11. Privacy and Data Protection	8
12. Anti-Harassment and Non-Discrimination	8
13. Anti-Retaliation.....	8
14. Ticket Handling Requirements for Employees	8
15. Recordkeeping and Evidence Preservation	8
16. Automation, AI, and Moderation Tools.....	8
17. Training and Awareness.....	9
18. Reporting and Escalation	9
19. Exceptions	9
20. Governance and Review	9
21. Related Documents.....	9
22. Standard Warning Language.....	9
23. External Notice for Ticket Portal	9
24. Legal and Compliance Positioning	10
Annex A – USA and UAE Compliance Cross-Reference Matrix	11
A1. Purpose and Definitions	11
Annex B – Support Agent SOP and Escalation Workflow.....	14
B1. Purpose	14

B2. Agent Rules	14
B3. Severity Guide	14
B4. De-escalation Steps	14
B5. Documentation Requirements	14
B6. Escalation Triggers	15
B7. Escalation Workflow	15
Annex C – Ticket Response Pack	16
C1. De-escalation	16
C2. First Warning	16
C3. De-escalation with Boundary	17
C4. Final Warning	17
C5. Refusal of Abusive Communication	17
C6. Escalation to Management	18
C7. Manager Follow-Up	18
C8. Controlled Communication / Cooldown	19
C9. Privacy / Personal Data Warning	19
C10. Threat / Safety Escalation Holding	19
C11. Quick-Select Guide	20
Appendix 1 – Primary Legal and Guidance Sources	21
Annex D – Communication Examples and Unacceptable Wording Guide	22
D1. Use of Examples	22
D2. No Personal Attacks	22
D3. No Hyperbolic Demands	22
D4. No Swearing or Profanity	23
D5. No Text Shouting	23
D6. Agent Handling Note	24

Document Control

Field	Details
Document Title	Professional Conduct & De-escalation Standard (PCDS) Policy
Document Number	PCDS-001
Version	1.0
Policy Owner	Compliance Department
Approved By	A Chief Compliance Officer (CCO)
Approval Date	1 August 2025
Effective Date	1 Jan 2026
Review Date	1 June 2026
Supersedes	New
Classification	Internal Policy / External Conduct Standard
Applicable Entities	All customers, service providers, employees, contractors, agents, and ticket-system users

Approval and Sign-Off

Role	Name	Signature	Date
Policy Owner	Compliance Department		
Legal Review	A Chief Legal Officer (CLO)		
Compliance Review	A Chief Compliance Officer (CCO)		
Executive Approver	An Executive Vice President (EVP)		

Professional Conduct & De-escalation Standard (PCDS) Policy

1. Purpose

1.1 This Policy establishes a professional, respectful, safe, and legally aware standard for communications exchanged through the Company's ticketing, support, complaint, helpdesk, and escalation systems.

1.2 It is designed to reduce abusive, aggressive, threatening, discriminatory, retaliatory, privacy-invasive, or otherwise unlawful conduct while supporting fair and efficient issue resolution.

1.3 This Policy applies equally to customers, service providers, employees, contractors, and authorized third parties using the ticket system.

2. Scope

2.1 This Policy applies to all communications sent, received, stored, reviewed, or escalated through support portals, email-to-ticket systems, chat transcripts converted into tickets, complaint portals, case notes, attachments, and escalation workflows.

2.2 It applies to internal and external users, including customers, end users, vendors, service providers, support agents, managers, moderators, investigators, and other authorized users.

3. Policy Statement

3.1 All users of the ticketing and support systems must communicate in a professional, respectful, factual, and non-threatening manner.

3.2 Disagreement, dissatisfaction, complaint escalation, and firm criticism are permitted. Abuse, threats, harassment, discrimination, coercion, extortion, privacy violations, and intimidation are prohibited.

3.3 The Company may moderate, warn, restrict, re-route, or escalate communications that violate this Policy while continuing to review legitimate underlying service issues through appropriate channels.

4. Guiding Principles

4.1 Professionalism: Communications must remain focused on facts, service issues, requested remedies, evidence, and documented next steps.

4.2 Mutual Respect: Customers and service providers are equally bound by this Policy.

4.3 De-escalation First: Where safe and appropriate, the Company will seek to calm and redirect communications before restricting them.

4.4 Safety and Compliance: Threats, harassment, extortion, discrimination, privacy violations, and other high-risk conduct require immediate intervention.

4.5 Fair Issue Resolution: A conduct violation does not automatically eliminate the Company's obligation to review a legitimate service issue in good faith.

5. Definitions

5.1 Abusive Communication means language or conduct that is insulting, degrading, obscene, threatening, intimidating, harassing, discriminatory, or otherwise inappropriate for a professional service environment.

5.2 Aggressive Communication means hostile, coercive, or intimidating language intended to pressure, demean, or alarm another person.

5.3 De-escalation means the use of neutral, professional, and structured communication intended to reduce tension and restore productive dialogue.

5.4 Protected Characteristic means any legally protected characteristic recognized under applicable law, including race, color, religion, sex, sexual orientation, gender identity, pregnancy, national origin, age, disability, or genetic information.

5.5 Personal Data means information relating to an identified or identifiable individual, including contact details, account data, complaint details, IDs, attachments, and other protected information.

6. Standards of Acceptable Conduct

6.1 All users must use respectful and professional language, state concerns factually and clearly, avoid personal attacks, and cooperate with reasonable requests for documents or clarification.

6.2 Employees and service providers must remain neutral and professional at all times, avoid sarcastic or retaliatory responses, and escalate deteriorating communications instead of arguing.

7. Prohibited Conduct

7.1 The following conduct is prohibited in any ticket, note, transcript, subject line, attachment, or escalation message: insults, slurs, ridicule, humiliation, degrading remarks, directed profanity, discriminatory remarks, threats of violence or retaliation, blackmail, extortion, bullying, harassment, sexual intimidation, doxxing, unauthorized disclosure of personal data, malicious false accusations, fabricated evidence, and repeated hostile message flooding.

7.2 The Company may determine, in its reasonable discretion, whether specific conduct violates this Policy and whether immediate restriction or escalation is required.

8. De-escalation Protocol

8.1 Step 1 – Pause and Review: The responder must review the message calmly and remove any reactive or emotional wording from the draft response.

8.2 Step 2 – Acknowledge: Recognize the concern in neutral language.

8.3 Step 3 – Reframe: Focus the conversation on facts, evidence, required actions, and available remedies.

8.4 Step 4 – Set Boundaries: If abuse appears, issue a formal conduct reminder.

8.5 Step 5 – Limit Engagement: If abuse continues, restrict handling to manager review, controlled updates, or a designated escalation channel.

8.6 Step 6 – Escalate High-Risk Conduct: Immediate escalation is required for threats, discriminatory harassment, extortion, privacy breaches, self-harm statements, or suspected criminal conduct.

9. Enforcement Levels

9.1 Level 1 – Minor Incivility: rude tone, impatience, disruptive formatting, or non-directed profanity. Possible actions include a reminder and redirection.

9.2 Level 2 – Direct Abuse: insults, targeted profanity, intimidation, or repeated hostile messages. Possible actions include formal warning, manager review, and communication controls.

9.3 Level 3 – Severe Misconduct: threats, discriminatory harassment, privacy violations, extortion, or continued abuse after warning. Possible actions include immediate restriction and escalation to Legal, Compliance, HR, Privacy, or Security.

9.4 Level 4 – Critical Risk: credible violent threats, severe data exposure, stalking, blackmail, or serious criminal conduct. Possible actions include emergency escalation and law-enforcement referral where appropriate.

10. Zero-Tolerance Categories

10.1 The following may result in immediate restriction or escalation without repeated warnings: credible threats of harm, hate speech, discriminatory harassment, sexual harassment, blackmail, extortion, publication of sensitive personal data, malicious defamatory allegations presented as fact without basis, and other unlawful content under applicable law.

11. Privacy and Data Protection

11.1 Ticket communications often contain Personal Data and must be handled using minimum-necessary principles and appropriate technical and organizational safeguards.

11.2 Users must not post passwords, full payment card details, government ID numbers, health information, or unrelated third-party personal data through standard ticket channels unless specifically required through an approved secure process.

11.3 Where excessive or inappropriate data is submitted, the Company may redact, restrict, or remove such data where lawful and operationally feasible.

12. Anti-Harassment and Non-Discrimination

12.1 The Company prohibits harassment and discriminatory conduct in all ticket-system communications.

12.2 No customer, client, vendor, contractor, employee, or agent may use the ticket system to target another person based on a protected characteristic.

13. Anti-Retaliation

13.1 No employee, service provider, or representative may retaliate against a person for raising a complaint in good faith or for reporting misconduct.

13.2 No customer or external user may retaliate against personnel for enforcing this Policy.

14. Ticket Handling Requirements for Employees

14.1 Employees must not match hostile tone, argue, mock, threaten personal consequences, disclose internal commentary confrontationally, or retaliate in any form.

14.2 Employees should use approved response templates, keep replies short and factual during conflict, and escalate rather than argue.

15. Recordkeeping and Evidence Preservation

15.1 The Company shall retain, according to applicable retention requirements, original ticket text, timestamps, attachments, warnings, restrictions, escalation notes, and relevant audit logs.

15.2 Serious threats, privacy breaches, and unlawful content must be preserved in a secure, tamper-resistant manner.

16. Automation, AI, and Moderation Tools

16.1 The Company may use automated tools to detect abusive or high-risk language.

16.2 Automated tools must not be the sole basis for final adverse action in high-risk matters without appropriate human review.

16.3 AI-generated or automated responses must remain professional, non-discriminatory, and policy-compliant.

17. Training and Awareness

17.1 Relevant personnel shall receive periodic training on professional communication standards, de-escalation, harassment recognition, privacy, incident escalation, and safe use of automated tools.

17.2 Training records should be maintained in accordance with Company practice.

18. Reporting and Escalation

18.1 Employees must report suspected violations of this Policy to the appropriate supervisor, Compliance, Legal, HR, Privacy, or Security function depending on severity.

18.2 Immediate escalation is mandatory for violent threats, discriminatory harassment, extortion, privacy or data exposure, and suspected criminal activity.

19. Exceptions

19.1 Any exception to this Policy must be approved in writing by the Policy Owner and, where appropriate, Legal and Compliance.

19.2 No exception may authorize unlawful conduct, unsafe practices, or avoidable privacy violations.

20. Governance and Review

20.1 The Policy Owner is responsible for implementation, maintenance, and periodic review of this Policy.

20.2 This Policy shall be reviewed at least annually or earlier if required by law, operational incidents, audits, litigation, or regulatory developments.

21. Related Documents

21.1 This Policy should be read together with the Customer Support SOP, Complaint Handling Procedure, Privacy Notice, Data Retention Policy, Information Security Policy, Anti-Harassment Policy, Employee Code of Conduct, and Incident Response Procedure.

22. Standard Warning Language

22.1 First Warning: "We are committed to helping resolve your issue. Please keep all communications respectful and professional. Insults, threats, discriminatory language, and abusive wording are not permitted in this ticket channel."

22.2 Final Warning: "We want to continue assisting you, but we cannot do so while the conversation includes abusive or threatening language. If this continues, the ticket may be restricted or escalated for safety, compliance, or legal review."

22.3 Restriction Notice: "Because this ticket includes prohibited conduct, communication on this matter is now restricted to the designated escalation channel. We will continue to review the underlying service issue under applicable policy."

23. External Notice for Ticket Portal

23.1 Recommended portal notice: "Please communicate respectfully and professionally. Abusive language, threats, discriminatory remarks, harassment, privacy violations, extortion, and unlawful content are prohibited. Messages may be moderated, restricted, or escalated for safety, compliance, or legal review."

24. Legal and Compliance Positioning

24.1 This Policy is intended to support a practical compliance baseline for U.S. and UAE operations. It is not, by itself, a substitute for legal advice or country-specific employment, privacy, consumer, cybercrime, or regulatory procedures.

24.2 For United States operations, relevant baseline considerations include workplace harassment, customer/client harassment, threats, privacy/security obligations, and fair/non-deceptive practices.

24.3 For United Arab Emirates operations, relevant baseline considerations include online insult and slander restrictions, privacy protections, cybercrime controls, media-content standards, and personal-data protection obligations.

Annex A – USA and UAE Compliance Cross-Reference Matrix

Field	Details
Annex Title	Annex A – USA and UAE Compliance Cross-Reference Matrix
Parent Policy	Professional Conduct & De-escalation Standard (PCDS) Policy
Parent Document Number	PCDS-001
Annex Document Number	PCDS-001-A
Version	1.0
Annex Owner	Compliance Department
Effective Date	1 Jan 2026
Next Review Date	1 June 2026
Classification	Internal Compliance Annex

A1. Purpose and Definitions

This Annex provides a formal cross-reference between each numbered PCDS Policy section and the principal legal/compliance considerations relevant to operations in the United States and the United Arab Emirates. It is an interpretive governance tool and not a substitute for legal advice.

- “U.S. Alignment” means the relationship between a PCDS provision and relevant U.S. legal, regulatory, or compliance considerations.
- “UAE Alignment” means the relationship between a PCDS provision and relevant UAE legal, regulatory, or compliance considerations.
- “Compliance Consideration” means a legal, regulatory, governance, risk, or operational issue that a policy section is intended to support, mitigate, or address.
- “Primary Source” means an official government or authoritative legal reference used to support the alignment described in this Annex.

PCDS Section	Control Theme	U.S. Alignment / Considerations	UAE Alignment / Considerations	Implementation Note	Primary Sources
1. Purpose	Safe, respectful, lawful communications	Supports prevention of harassment, threats, retaliation, unfair handling, and privacy/security failures.	Supports lawful online conduct, privacy protection, and content-control expectations.	Use as umbrella justification for conduct, safety, and privacy controls.	EEOC; FTC; UAE Cyber Safety
2. Scope	Broad application across users and channels	Important because customers, clients, and non-employees may be sources of unlawful harassment in workplace settings.	Important because online conduct risks may arise across all digital channels and participants.	Ensure tickets, portal notes, chats, emails, and attachments are included.	EEOC Small Business Fact Sheet; UAE Media Regulation
3. Policy Statement	Professional, respectful, non-threatening communication	Consistent with anti-harassment, threat avoidance, and fair business conduct principles.	Consistent with restrictions on insulting, slandering, invasive, and harmful digital communications.	Maintain distinction between company policy violation and legal violation.	EEOC; FTC Enforcement; UAE Cyber Safety
4. Guiding Principles	Professionalism, mutual respect, de-escalation, safety	Supports prompt corrective action and governance reasonableness.	Supports responsible digital conduct and privacy-aware interactions.	Useful for training and audit narrative.	EEOC; UAE Media Regulation
5. Definitions	Operational definitions	Helps distinguish ordinary incivility from protected-status harassment and privacy-sensitive data.	Helps distinguish general frustration from insult, slander, privacy invasion, and unlawful online conduct.	Keep definitions consistent with SOPs.	EEOC Small Business Fact Sheet; UAE PDPL

6. Standards of Acceptable Conduct	Required respectful behavior	Supports fair, non-retaliatory, professional handling of disputes.	Supports lawful, respectful ticket communication and controlled resolution channels.	Use as front-line handling standard.	EEOC; FTC Enforcement; UAE Cyber Safety
7. Prohibited Conduct	Insults, threats, slurs, extortion, doxxing	Relevant to protected-status harassment, threats, extortion, and malicious conduct; threats may implicate federal law.	Direct relevance to insult, slander, defamation, blackmail, privacy invasion, and harmful online content.	Core moderation rule set.	18 U.S.C. §875; UAE Cyber Safety; UAE Media Regulation
8. De-escalation Protocol	Structured response to heated communications	Supports prompt and appropriate corrective action and reduces retaliation/escalation risk.	Supports proportionate moderation and controlled response to unsafe digital content.	Operationalize in SOP and agent scripts.	EEOC; UAE Cyber Safety
9. Enforcement Levels	Graduated warning and restriction system	Demonstrates proportionality and consistency, useful in disputes and audits.	Demonstrates controlled and reasonable moderation response.	Keep decision logs for each enforcement level.	FTC Enforcement; UAE Media Regulation
10. Zero-Tolerance Categories	Immediate action for severe misconduct	Strong alignment for threats, discrimination, severe harassment, and sensitive data misuse.	Strong alignment for blackmail, privacy invasion, insult/slander, unlawful content, and safety risk.	Reserve for clearly high-risk categories.	18 U.S.C. §875; EEOC; UAE Cyber Safety
11. Privacy and Data Protection	Minimum necessary data, secure handling, limited disclosure	Directly aligned with FTC expectations for data security and honoring privacy commitments.	Directly aligned with UAE PDPL confidentiality, security, purpose limitation, and data-subject rights.	Pair with privacy notice, retention rules, and access controls.	FTC Privacy & Security; UAE Data Protection Laws; UAE PDPL
12. Anti-Harassment and Non-Discrimination	No harassment based on protected characteristics	Direct EEOC relevance for hostile or abusive conduct tied to protected characteristics.	Also supports UAE restrictions relating to discrimination, racism, and contempt of religion in online content controls.	Keep this section explicit for U.S. employment compliance.	EEOC; UAE Media Regulation
13. Anti-Retaliation	No retaliation for complaints or enforcement	Important control where users or employees report misconduct.	Supports fairness and disciplined governance even where the legal structure differs.	Document legitimate reasons for action.	EEOC Small Business Fact Sheet
14. Employee Handling Requirements	Agents remain neutral and do not match tone	Supports non-retaliatory and professional response practices.	Reduces risk of unlawful or inappropriate digital conduct by staff.	Use standard templates and escalation rules.	EEOC; UAE Cyber Safety
15. Recordkeeping and Evidence Preservation	Preserve tickets, warnings, logs, and evidence	Important for harassment investigations, privacy incidents, disputes, and threat review.	Important for cyber, privacy, and complaint investigations and proof of message history.	Use secure, tamper-resistant logging where possible.	FTC Privacy & Security; UAE PDPL; 18 U.S.C. §875
16. Automation, AI, and Moderation Tools	Human review and controlled automation	Supports fairness and reduces risk of inaccurate or unfair automated moderation.	Relevant to UAE data-processing safeguards and human review concerns.	High-risk actions should receive human review.	FTC Enforcement; UAE PDPL
17. Training and Awareness	Training on conduct, escalation, privacy	Strong preventive governance support under U.S. harassment and compliance frameworks.	Supports implementation of privacy, cyber, and content-control requirements.	Maintain training records.	EEOC Small Business Fact Sheet; FTC Privacy & Security; UAE Data Protection Laws
18. Reporting and Escalation	Escalation to legal, HR, compliance, security	Needed for prompt corrective action, threat response, and investigations.	Needed for online abuse, privacy, extortion, and harmful content response.	Build routing decision trees.	EEOC; 18 U.S.C. §875; UAE Cyber Safety
19. Exceptions	Formal approval for policy exceptions	Supports governance, fairness, and prevention of arbitrary departures.	Supports governance discipline and controlled deviation management.	Require written Legal/Compliance approval.	FTC Enforcement; UAE PDPL
20. Governance and Review	Annual review and update controls	Good compliance hygiene and ongoing adequacy review.	Same principle applies for evolving cyber/data compliance needs.	Put on annual compliance calendar.	FTC Privacy & Security; UAE Data Protection Laws

21. Related Documents	Links to SOPs, privacy, security, retention	Compliance requires cross-functional documentation, not one policy alone.	Compliance also depends on connected operational documents and controls.	Link by document number where possible.	FTC Privacy & Security; UAE PDPL
22. Standard Warning Language	Controlled warning templates	Helps avoid retaliatory, inflammatory, or inconsistent staff wording.	Helps keep moderation language neutral and professional.	Centralize templates in SOP or knowledge base.	EEOC; UAE Media Regulation
23. External Notice for Ticket Portal	Customer-facing conduct notice	Supports fair notice, moderation transparency, and enforceability.	Supports notice that prohibited digital conduct may be restricted or escalated.	Display at submission, reply, and escalation screens.	FTC Enforcement; UAE Cyber Safety
24. Legal and Compliance Positioning	Baseline alignment, not legal advice	Important so policy is not read as exhaustive legal guidance or legal guarantee.	Important for same reason, especially where sector-specific rules may apply.	Retain disclaimer in final approved version.	FTC Enforcement; UAE Data Protection Laws

Annex B – Support Agent SOP and Escalation Workflow

Field	Details
Document Number	PCDS-SOP-01
Version	1.0
Owner	Customer Support / Compliance
Effective Date	1 Jan 2026
Applies To	All support agents, team leads, QA reviewers, managers, and escalation teams

B1. Purpose

This SOP instructs support agents how to identify, de-escalate, document, and escalate aggressive, abusive, threatening, discriminatory, or privacy-risk communications in the ticket system.

B2. Agent Rules

- Remain calm, neutral, and professional.
- Never match tone, argue, mock, threaten, or retaliate.
- Focus on facts, next steps, and boundaries.
- Preserve evidence accurately and completely.
- Escalate immediately if safety, discrimination, privacy, extortion, or legal risk appears.

B3. Severity Guide

Level	Description	Examples	Required Agent Action
A	Frustrated but manageable	Caps lock, impatience, repeated complaints, rude tone, non-directed profanity	Acknowledge, reframe, resolve, and document if pattern repeats
B	Abusive	Direct insults, targeted profanity, humiliation, intimidation, repeated hostile messages	Issue formal warning, continue only if communication stabilizes, escalate if repeated
C	High-risk / immediate escalation	Threats, discriminatory slurs, sexual harassment, blackmail/extortion, doxxing, data exposure, self-harm statements	Stop normal handling immediately, preserve evidence, escalate to Team Lead + Compliance/Legal/Security

B4. De-escalation Steps

- Step 1 – Pause: Do not reply emotionally; remove reactive wording from the draft.
- Step 2 – Acknowledge: Use one calm statement, such as “I understand this situation is frustrating.”
- Step 3 – Reframe: Convert emotion into an operational issue and specify the next required action.
- Step 4 – Set Boundary: If direct abuse appears, issue the approved formal warning.
- Step 5 – Restrict if Needed: Move to manager-only response, written-only handling, or controlled cadence if abuse continues.

B5. Documentation Requirements

- Ticket number, date/time, exact abusive language or conduct category, severity level, warning issued, screenshot or attachment reference, customer request summary, agent response summary, escalation destination, and restriction applied.
- Do not loosely paraphrase threats or discriminatory language in internal notes. Preserve the original text accurately.
- Handle ticket records securely because they may contain Personal Data.

B6. Escalation Triggers

- Threat of violence or injury
- Blackmail or extortion
- Discriminatory or sexual harassment
- Doxxing or disclosure of personal/confidential data
- Self-harm or harm-to-others statements
- Stalking behavior
- Suspected fraud, forged evidence, or criminal conduct
- Repeated abuse after formal warning

B7. Escalation Workflow

Ticket Received → Review message content → Level A (Frustrated/Rude Only): Acknowledge + Reframe + Resolve issue; document if pattern repeats. Level B (Direct Abuse/Targeted Insults): Issue formal warning. If conduct stops, continue with controlled professional handling; if it continues, restrict contact and escalate to Team Lead/Manager. Level C (Threat/Discrimination/Extortion/Privacy Breach): Stop normal handling immediately, preserve evidence exactly, escalate to Team Lead + Compliance/Legal/Security, and apply authorized restrictions.

Trigger	First Escalation	Secondary Escalation	Agent Action
Rude / angry but not abusive	Team Lead if repeated	QA / Manager	De-escalate and continue
Direct insults / targeted profanity	Team Lead	Manager	Warn, document, restrict if repeated
Discriminatory harassment	Manager	HR / Compliance / Legal	Stop normal handling and escalate immediately
Threat of violence / injury	Manager	Security / Legal	Immediate escalation and evidence preservation
Blackmail / extortion	Manager	Legal / Security	Do not negotiate; escalate immediately
Privacy breach / doxxing / sensitive data exposure	Manager	Privacy / Compliance / Security	Restrict access and preserve evidence
Self-harm / harm-to-others	Manager	Security / Emergency Protocol	Immediate escalation per crisis procedure

Annex C – Ticket Response Pack

Field	Details
Document Number	PCDS-TMP-01
Version	1.0
Owner	Customer Support / Compliance
Purpose	Ready-to-use response messages for de-escalation, warnings, restriction, and escalation
Placeholders	[Customer Name], [Ticket Number], [Issue Summary], [Required Action], [Timeframe], [Escalation Channel], [Manager Name / Team], [Company Name]

C1. De-escalation

Subject: Re: Ticket [Ticket Number] – [Issue Summary]

Dear [Customer Name],

I understand this situation is frustrating, and I want to help move it toward resolution.

To keep this process moving, let us focus on the specific issue and the next step required. At this stage, we need [Required Action] in order to continue reviewing your request.

Once we receive that information, we will review the matter and update you by [Timeframe].

Thank you for your cooperation.

Kind regards,
[Agent Name]
AIH Support Team

C2. First Warning

Subject: Conduct Reminder – Ticket [Ticket Number]

Dear [Customer Name],

We are committed to helping resolve your issue. However, we ask that all communication in this ticket remain respectful and professional.

Insults, threats, discriminatory remarks, and abusive language are not permitted in this support channel. To continue assisting you, please keep future messages focused on the service issue and the requested resolution.

If you would like us to proceed, please send [Required Action], and we will continue our review by [Timeframe].

Kind regards,
[Agent Name]
AIH Support Team

C3. De-escalation with Boundary

Subject: Re: Ticket [Ticket Number] – Next Step Required

Dear [Customer Name],

I understand that you are dissatisfied with the current situation. We are prepared to continue assisting you, but we need the conversation to remain professional.

Please avoid insults, threats, or abusive wording in further messages. The fastest way to move this matter forward is to focus on the issue itself, which is [Issue Summary].

The next step required from you is [Required Action]. Once received, we will review and respond by [Timeframe].

We appreciate your cooperation.

Kind regards,
[Agent Name]
AIH Support Team

C4. Final Warning

Subject: Final Conduct Warning – Ticket [Ticket Number]

Dear [Customer Name],

We want to continue assisting you with [Issue Summary]. However, your recent messages have continued to include language that does not comply with our communication standards.

This is a final warning. If abusive, threatening, discriminatory, or otherwise inappropriate communication continues, this ticket may be restricted, reassigned, or escalated for management and compliance review.

We remain available to review the underlying issue if future communication stays respectful and focused on the matter to be resolved. If you wish to proceed, please provide [Required Action].

Kind regards,
[Agent Name]
AIH Support Team

C5. Refusal of Abusive Communication

Subject: Communication Restricted – Ticket [Ticket Number]

Dear [Customer Name],

We are unable to continue the current discussion in its present form because recent messages in this ticket contain abusive, threatening, discriminatory, or otherwise inappropriate communication.

Effective immediately, normal back-and-forth communication on this ticket is being restricted. We will continue to review the service issue through the appropriate process, but future communication must remain respectful and professional.

If permitted under our process, any further updates will be provided through [Escalation Channel].

Kind regards,
[Agent Name]
AIH Support Team

C6. Escalation to Management

Subject: Ticket Escalated for Management Review – [Ticket Number]

Dear [Customer Name],

Your ticket has been escalated to [Manager Name / Team] for further review. This escalation has been made due to the nature of the recent communications and/or the need for additional oversight on the matter.

The underlying issue, [Issue Summary], remains under review. Any further updates will be provided through [Escalation Channel] within [Timeframe].

Please note that all future communication must remain respectful and professional to allow the review process to continue efficiently.

Kind regards,
[Agent Name]
AIH Support Team

C7. Manager Follow-Up

Subject: Management Review in Progress – Ticket [Ticket Number]

Dear [Customer Name],

I am writing as the assigned reviewer for this matter following escalation of your ticket. I have reviewed the case history and the recent communications.

We are prepared to continue reviewing the service issue; however, communication in this matter must remain respectful, factual, and professional. Abusive or threatening language will not be accepted.

To proceed, please provide [Required Action], if still outstanding. We will issue the next update by [Timeframe].

Regards,
[Manager Name]
[Title]
AIH

C8. Controlled Communication / Cooldown

Subject: Controlled Communication Process – Ticket [Ticket Number]

Dear [Customer Name],

To help manage this matter constructively, communication on this ticket will now proceed through a controlled process. We will review all incoming messages and provide one consolidated response within [Timeframe / e.g., one business day].

This measure is being applied to maintain a professional and productive review process. We remain willing to address the underlying issue, provided communications remain respectful and focused on the case.

Kind regards,
[Agent or Manager Name]
AIH

C9. Privacy / Personal Data Warning

Subject: Sensitive Information Notice – Ticket [Ticket Number]

Dear [Customer Name],

For your security and privacy, please do not send passwords, full payment card details, government identification numbers, or unrelated third-party personal information through this ticket channel unless specifically requested through an approved secure process.

If additional documentation is required, we will provide the correct secure submission method. Please resend only the minimum information necessary for us to review your request.

Kind regards,
[Agent Name]
AIH Support Team

C10. Threat / Safety Escalation Holding

Subject: Ticket Under Formal Review – [Ticket Number]

Dear [Customer Name],

Your recent communication has been placed under formal review. Due to the nature of the content received, this matter has been referred to the appropriate internal team for assessment.

We will not continue standard ticket handling until that review is completed. If further communication is accepted, it must remain professional and limited to the service issue.

Regards,
[Agent / Manager Name]
AIH

C11. Quick-Select Guide

Situation	Recommended
Customer is angry, demanding, or rude but still manageable	De-escalation
First direct insult or targeted profanity	First Warning
Customer is emotional and abusive but still possibly recoverable	De-escalation with Boundary
Abuse continues after first warning	Final Warning
Abuse continues and agent must stop direct engagement	Refusal of Abusive Communication
Ticket must be moved to team lead or manager	Escalation to Management
Manager takes control of case	Manager Follow-Up
High conflict requires reduced message frequency	Controlled Communication / Cooldown
Sensitive personal data is posted	Privacy / Personal Data Warning
Threat, extortion, or serious safety issue	Threat / Safety Escalation Holding

Appendix 1 – Primary Legal and Guidance Sources

- U.S. Equal Employment Opportunity Commission – Harassment: <https://www.eeoc.gov/harassment>
- U.S. Equal Employment Opportunity Commission – Small Business Fact Sheet: Harassment in the Workplace: <https://www.eeoc.gov/small-business-fact-sheet-harassment-workplace>
- Federal Trade Commission – Privacy and Security: <https://www.ftc.gov/business-guidance/privacy-security>
- Federal Trade Commission – Enforcement Authority: <https://www.ftc.gov/about-ftc/mission/enforcement-authority>
- 18 U.S. Code # 875 – Interstate Communications: <https://www.law.cornell.edu/uscode/text/18/875>
- The Official Platform of the UAE Government – Cyber Safety and Digital Security: <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security>
- The Official Platform of the UAE Government – Media Regulation: <https://u.ae/en/media/media-in-the-uae/media-regulation>
- The Official Platform of the UAE Government – Data Protection Laws: <https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws>
- UAE Legislation – Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data: <https://uaelegislation.gov.ae/en/legislations/1972>

Annex D – Communication Examples and Unacceptable Wording Guide

This annex provides practical examples for support agents, managers, and moderators to identify language patterns that violate the Professional Conduct & De-escalation Standard (PCDS). These examples are illustrative and are intended to support consistent moderation, coaching, and escalation decisions. Where possible, agents should redirect the sender toward a neutral and issue-focused alternative.

D1. Use of Examples

The examples below are not exhaustive. Similar wording, tone, or formatting may also be restricted if it creates a hostile, abusive, aggressive, or unprofessional communication environment. The “Preferred Professional Alternative” column is provided as a guide for how the concern may be expressed in an acceptable way.

D2. No Personal Attacks

Personal attacks target the person instead of the issue. They include insults, humiliation, ridicule, degrading remarks, or statements intended to belittle the other party.

No.	Unacceptable Example	Preferred Professional Alternative
1	"You are incompetent and clearly do not know how to do your job."	"I do not believe my issue has been handled correctly. Please review it again."
2	"Your team is useless."	"I am dissatisfied with the support outcome and would like escalation."
3	"Only an idiot would respond like this."	"This response does not address my concern. Please clarify the reasoning."
4	"You people are hopeless."	"I am concerned that my issue is still unresolved."
5	"The agent handling this is a joke."	"I do not think the handling has met my expectations."
6	"Are you even capable of reading my messages?"	"Please confirm you have reviewed the information I previously submitted."
7	"This is the dumbest support team I have ever dealt with."	"This has been one of the most difficult support experiences I have had."
8	"You are lying to me."	"I believe the information provided may be inaccurate. Please verify it."
9	"You must be clueless."	"I believe there may be a misunderstanding about the issue."
10	"Your manager should fire you."	"I would like this case reviewed by a manager."

D3. No Hyperbolic Demands

Hyperbolic demands use exaggerated, coercive, or absolute language that is intended to pressure the other party rather than move the issue toward a reasonable resolution.

No.	Unacceptable Example	Preferred Professional Alternative
1	"Fix this right now or I will destroy your company online."	"Please treat this as urgent and confirm the next step today."
2	"I want a full resolution in 5 minutes."	"Please let me know the soonest realistic resolution time."
3	"If this is not solved immediately, there will be consequences."	"If this cannot be resolved quickly, please escalate it to management."
4	"I expect every penny refunded today, no excuses, no delay, no exceptions."	"I am requesting a refund and would like to know the applicable review timeline."
5	"Your company must drop everything and prioritize me now."	"Please prioritize this case if possible due to its urgency."
6	"I need this fixed instantly or I am taking legal action today."	"If this cannot be resolved internally, please advise me of the formal escalation process."

7	"You must answer every message within 10 minutes."	"Please confirm your expected response time for this ticket."
8	"I demand a senior executive call me immediately."	"Please escalate this matter to a manager or senior reviewer."
9	"Do whatever it takes and solve this today no matter what."	"Please explain what options are available to resolve this today, if possible."
10	"I will not accept anything except an immediate total reversal of your decision."	"I disagree with the decision and request a formal review or appeal."

D4. No Swearing or Profanity

Swearing or profanity is not permitted when directed at a person, team, or company representative, or when it contributes to an abusive tone. For training purposes, some examples below are partially masked.

No.	Unacceptable Example	Preferred Professional Alternative
1	"This is bull****."	"I strongly disagree with this outcome."
2	"Your answer is complete sh**."	"Your answer does not resolve my concern."
3	"What the hell is wrong with your team?"	"Please explain why this issue has not yet been resolved."
4	"This f***ing process is ridiculous."	"This process feels unreasonable and I would like clarification."
5	"You are being damn useless."	"I do not think this response has been helpful."
6	"I am sick of this crap."	"I am very frustrated with the delay in resolving this issue."
7	"Stop sending me this nonsense crap."	"Please send only the information relevant to resolving my case."
8	"This whole thing is a damn mess."	"This situation appears disorganized and needs clarification."
9	"Why do I have to deal with this stupid sh**?"	"Why is this additional step required? Please explain."
10	"Your company handled this like crap."	"I am dissatisfied with how this matter has been handled."

D5. No Text Shouting

Text shouting includes full-sentence ALL CAPS, repeated aggressive capitalization, or excessive punctuation such as more than three exclamation points. These patterns may be treated as aggressive or intimidating when used in ticket communications.

No.	Unacceptable Example	Preferred Professional Alternative
1	"THIS IS UNACCEPTABLE AND YOU NEED TO FIX IT NOW."	"This is unacceptable to me, and I would like prompt assistance."
2	"WHY IS NOBODY HELPING ME???!!!"	"Why has my issue not yet been addressed?"
3	"I HAVE SENT THIS THREE TIMES ALREADY!!!"	"I have already sent this information three times."
4	"DO NOT IGNORE ME AGAIN!!!"	"Please confirm receipt and next steps."
5	"I WANT A REFUND RIGHT NOW!!!!!"	"I am requesting a refund as soon as possible."
6	"YOUR TEAM NEVER DOES ANYTHING CORRECTLY!!!"	"I am dissatisfied with the quality of support I have received."
7	"ANSWER ME TODAY OR ELSE!!!"	"Please provide an update today if possible."
8	"THIS MAKES NO SENSE AT ALL!!!"	"This explanation is unclear to me. Please clarify."
9	"I ALREADY TOLD YOU EVERYTHING YOU NEED TO KNOW!!!"	"I believe I already provided the necessary information."
10	"STOP WASTING MY TIME AND FIX IT!!!!!"	"Please focus on resolving the issue as efficiently as possible."

D6. Agent Handling Note

When an agent sees one or more of the example patterns above, the agent should classify the message under the applicable severity level in the SOP, preserve the relevant text accurately, issue the correct warning or boundary message where appropriate, and escalate according to the approved workflow if the conduct is repeated or high-risk.