MANAV RACHNA UNIVERSITY
Declared as State Private University vide Haryana Act 26 of 2014

MANAV RACHNA UNIVERSITY

(Established vide Haryana Act 26 of 2014)

MINUTES

OF

SEVENTEENTH MEETING

OF THE

BOARD OF MANAGEMENT

Dated: 07.08.2021

MINUTES OF THE SEVENTEENTH MEETING OF THE BOARD OF MANAGEMENT OF MANAV RACHNA UNIVERSITY HELD ON SATURDAY, DATED 07-08-2021 AT 11.00 A.M IN BOARD ROOM A-BLOCK MR CAMPUS

17th meeting of the Board of Management of Manav Rachna University was held on Saturday, Dated 07-08-2021 at 11.00 A.M in Board Room, A Block, MR Campus to consider various administrative, financial and academic matters. The following were present:

1. Prof. I.K. Bhat, Vice Chancellor
2. Dr. Amit Bhalla, Vice President, MREI
3. Dr. M.M. Kathuria, Trustee, UET
4. Dr. N.C. Wadhwa, DG, MREI (Special Invitee)
5. Dr. Shalini Tuli, Associate Professor (Nominee of Govt. of Haryana);
6. Prof. (Dr) V.K. Mahna, Ex-PVC, MRU.
7. Prof. Sangita Banga, Dean, Academics;
8. Prof. Pradeep K. Varshney, Dean, Research;
9. Prof. Parul Jhajharia, Dean, Mgt. & Com (Special Invitee)
10. Prof. Shruti Vashisht, Dean, SW & HoD, ECE
11. Dr. Kameshwar Singh, Registrar/ Member Secretary

Prof. Jyoti Pruthi, Associate HoD, CST, Prof. Versha Vahini, Associate Dean & HOD, Law, Shri Rajiv Kapoor, ED; Group HR, Head, Uno Minda and Shri. Navdeep Chawla, Chairman/MD, Psychotropic India Ltd could not attend the meeting due to their other professional engagements; they were granted leave of absence.

The following are the minutes of the meeting:

Registrar welcomed the Hon'ble Members and briefed them about the agenda to be deliberated in the meeting. The Chairman was then requested to open the meeting with his remarks.

1. Opening Remarks by the Chairman

Chairman welcomed all the members, especially external members, for taking out time to attend the meeting and hoped that their presence would help in deliberating on some of the important issues which the university finds important to report to the Board of Management and seek their advice on the same. He further stated that a lot of activities have been carried out since last BOM Meeting, which relates to academics, research, innovations and other students related matters.

The Vice Chancellor informed the respected members about the same and some of the important one are listed below:

(i). Manav Rachna Educational Institutions (MREI) have entered into its 25th year of academic journey and to commemorate the occasion. Year-long silver jubilee celebrations started with a webinar on "THE MESSAGE OF THE BHAGVAD GITA" by Dr. Karan Singh on 8th July 2021.

(ii). The Academic Council meeting was held on 20.07.2021 and some of the recommendations are presented in today's agenda notes.

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

(iii). As per Times Engineering survey 2021, Faculty of Engineering, MRU has been ranked as the 2nd top-most emerging institute and is top-most in terms of employability & research capabilities.

(iv). MRU has received the extension of approval for all its B. Tech and M. Tech programs for the academic year 2021-22. MRU had applied for change in nomenclature for B. Tech Electronics & Computers to Electronics & Communications and the same has been approved by AICTE.

(v). The MRNAT phase 1 was conducted on 23rd & 24th May and MRNAT Phase II conducted on 10th & 11th July and till date 175 (as on 6th August) students have taken admission in various programmes and the process will remain open till last dates as per the guidelines provided by UGC & AICTE.

(vi). Results have been declared for all higher semesters, including the second semester for which examinations were conducted in the month of July 2021.

(vii). University completed the even semester for all semesters including 2nd sem. for the 2020 batch and has started the classes for academic year 2021-22 for all existing students from 19th July in online mode and is planning to call students for physical classes in phased manner from 9th August 2021.

(viii). This year, PhD admissions were shifted from Dec-Jan to June-July session. On 18th July the total applications received were 223 applications. Total of 164 candidates appeared for entrance & Interview and result for PhD admissions under various Faculties have been declared on 2nd August 2021. In the final selection 75 candidates have been given admission this year in different programs.

(ix). Seven (7) research scholars have completed their final evaluation for the PhD work during last six months and six (6) are under the process of evaluation. Ten (10) more scholars are expected to submit thesis in next few months time.

(x). Department of CST organized two days international conference, "Computational Intelligence in Analytics & Information Systems" (CIAIS 2021), in hybrid mode on 1st & 2nd April 2021 which was a great success and all the papers were checked for plagiarism using Easy Chair and Turnitin and only 40% papers were selected for presentation & publication. Total 63 technical papers were presented during 10 technical sessions and 500 participants joined virtually & physically.

(xi). Department of ECE organized five days FDP on IOT & sensors from 26th July to 30th July. Experts from industry and academia delivered the sessions and was well received.

(xii). Manav Rachna Center for Peace & Sustainability is in the process of setting up Peace ZONE. Space for the same has been identified and necessary arrangements are being made to start it at an earliest.

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

(xiii). Manav Rachna Centre for Peace and Sustainability, in collaboration with Bombay Natural History Society organized a webinar on "Ecological Restoration: Growing Native Plants of Aravali. The session was delivered by Mr. Sohail Madaan from BHNS.

(xiv). Faculty of Law in collaboration with Bar and Bench & Suveeksha Eduskills offered 10 weeks online certification course on "Comparative Competition Law" from 4th June 2021 onwards.

(xv). Center of Legislative Studies & Research, Faculty of Law in collaboration with Suveeksha Eduskills offered 4 days online certification course on "Legislative Drafting" in March 2021. Twenty six (26) Candidates (both students and professionals) attended the course.

(xvi). Dr. Babita got the opportunity to launch 3 weeks MOOC course under UNESCO Mentoring program on "Social Emotional Learning: Learning to be".

(xvii). Prof. Pradeep K. Varshney was invited as a speaker to deliver a talk on "Business Intelligence" of IIMT, Greater Noida on 16 June 2021. He was also invited as a speaker to deliver a talk on "Alignment of Research and Innovation activities towards Sustainable Development Goals (SDGs)" in 3rd International Conference on Recent Trend on Science and Technology (ICRTST-2021) on June 19, 2021.

(xviii). Mr. Sudhir Singh of ME department successfully completed 4 months certification program in different modules like Tableau, Python, ML, SQL

(xix). Mr. Joginder Singh of Mechanical Engg department successfully completed the NPTEL Online Certification of "Processing of Polymers and Polymer Composites" with a consolidated score of 94%. He was in Top 5% of registered candidates and received the Gold Medal. This was an AICTE approved 8 weeks FDP course.

(xx). Mr. Piyush Mahendru & Mr. Sudhir Singh has successfully completed 5 days Faculty Development Program- Student Induction on UHV conducted online during 24 - 28 May 2021.

(xxi). Dr. Mrinal Pandey, mentored a project under the use-case titled 'Real-time price discovery & volume management at e-market places' which won first prize for AI grand challenge announced by CDAC Kolkata. The event was organised by Telangana government in Telangana AI Mission Agriculture AI Grand Challenge -2021.

(xxii). Ms. Gaganjot Kaur, Dept of CST dept received Mentor certificate for the Jan-Dec 2020 semester for IOT course on 24th March 2021 from NPTEL.

(xxiii). Dr. Sanjay Singh chaired a session at "International Conference on Intelligent Technologies (CONIT 2021), 25 – 27 June 2021, IEEE 2021 The International Conference for Intelligent Technologies, Hubballi, Kartakata, India.

(xxiv). Dr. Jyoti Pruthi has been appointed review for the journal "The Editors of Neuro-computing".

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

(xxv). Dr. Megha Bansal, was Invited at National Council of Cement and Building Materials as a Guest of Honour in the International Women's Day celebrations at NCCBM to address the officials and staff of NCCBM.

(xxvi). Dr. Manpreet Kaur, Dept of CST dept. has been elevated to "Senior Member" IEEE Award on 20th April by IEEE (USA) for her contribution and association with IEEE for student activities.

(xxvii). IEEE Delhi section felicitated student chapters from Delhi, Rajasthan, Punjab: Dr. Manpreet Kaur, past Chairperson Women in Engineering, has been felicitated with "Honorary WIE Recognition" award for her contribution as Chairperson, WIE Affinity Group, IEEE Delhi Section in 2020-2021.

(xxviii). Ms. Chaitali Wadhwa, was invited to be an Arbitrator Judge in the Moot Shanghai from 8-12 March 2021.

(xxix). Dr. Arpit Sand Delivered talk in one week short term course on theme 'Advanced Materials For Aatmanirbhar Bharat' in organized by J C Bose University of Science and Technology

(xxx). Mr. Sanjay Taneja published an article on "Blooming of Startup culture in India". In Haryana Magzine.

The Chairman also apprised the Board about the achievements of the University in Research Publications & placement:

- Mr. Prashant Bhardwaj has published a research paper on "Remaining Useful Life Estimation by Stochastic Markov Model and Monte-Carlo Simulation" in International Journal of Industrial & System Engineering.

- Dr. Sujata Nayak and Mr. Prashant Bhardwaj has published a research paper on "Enviro Economic and Energy matrices Analysis of semi-transparent PVT solar dryer integrated with kitchen chimney" on International Conference on Sustainable Engineering.

- Dr. Sujata Nayak and Mr. Prashant Bhardwaj published a research paper on "Design and Simulation of a semi-transparent photovoltaic thermal (PVT) indirect solar dryer integrated with kitchen chimney using ANN technique" in International Conference on Sustainable Engineering.

- Mr. Pradeep Kr Mouria published a research paper on "Measurement of residual stress on H13 tool steel during machining for fabrication of FSW/FSP tool pins" in Materials Today published by Elsevier.

- Dr. Sujata Nayak published a research Paper on "Impact of process variables on surface roughness in negative incremental forming process". Materials Today: Proceedings. Accepted 22 June 2021.Elsevier.

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

Placements

Placement process for the 2021 Batch is in progress. The department wise placement position is as follows:

- Harshit Aggarwal of CST got placed with Urvija AI at the package of 32 LPA
- Nandini Chauhan of CST has been selected for Fellowship with Teach for India and has also got admission at the Columbia Business School, New York.
- Srushti Suresh of CST got admission in University of San Francisco, USA for Masters of Management in Information Systems clearing GRE and IELTS
- In Department of CST 105 students out of 156 eligible candidates got placed in different companies.
- In Dept. of ME, 07 students have also got placed in core companies with Salary package : 5.07 LPA offered by DYSON INDIA
- In Dept. of Mathematics, 01 B.Sc. student was placed with a package of 10 LPA by LIDO LEARNING
- In Dept. of Chemistry 04 M.Sc. student placed with Salary Package: 3.8 LPA offered by Infollion Research Services (Average Salary Package: 2.8 LPA)
- In Dept. of Mgt. & Com. 5 students of BBA Program placed with salary package: 4 LPA offered by LIDO LEARNING.
- In Dept. of Education, 4 students of B.Ed. Program got placed.

"Some major/ remarkable Student Achievements

- IEEE MRU Student Branch has been honored with prestigious awards for outstanding work in 2020, in IEEE Delhi Section Annual Award Ceremony 2021, organized virtually at Delhi Technological University, on 4th July. They were acknowledged by IEEE Delhi Section Chairperson, under Student activity center (SAC).
- Mr. Rahul Thakur, student of B.Tech. CSE 8th Sem has been recognized as NPTEL Discipline Star for his **Six MOOC** Courses in Computer Science and Engineering Discipline where each course ranged between 8 to 12 weeks. The certificate of recognition has been awarded to him by SWAYAM-NPTEL (The National Programme on Technical Enhanced Learning).
- Mr. Parag Kumar Garg, student of B.Tech. CSE 8th Sem. has been recognized as NPTEL Discipline Star. He completed **Eight MOOC** Courses in Computer Science & Engineering Discipline where each course ranged between 8 to 12 weeks. The certificate of

recognition has been awarded to him by SWAYAM-NPTEL (The National Programme on Technical Enhanced Learning).

- Mayank Saxena, student of B.Tech. CSE with Data Science & Amp; Machine Learning 4th Sem got the opportunity of Intern (Graphic Designer) with Xebia.

- An article entitled 'Why Entrepreneurship is a Solution for Unemployment' authored by Mr. Shrey Bisht, student of B.Sc.(H) Mathematics (2020 – 23) II semester, was published in the eighth edition of MERAKI. It aims to spread awareness on Sustainable Development Goals (SGDs).

Chairman also briefed the Members about the activities carried out by the Department of Student Welfare, MRU during the past 5 months as follows:

- ✓ On the occasion of International Women's Day, Manav Rachna Peace and Sustainability Club in collaboration with The Department of Student Welfare and OP Bhalla Foundation organized a one weeklong celebration for International Women's day: "Adya". Eight different events were conducted under this agenda like Know Your Rights, Law Dialogue, Panel Discussion, Dare 2 Aspire, etc.

- ✓ On WATER DAY (22nd March) Manav Rachna Centre for Peace and Sustainability, MRU; Department of Student Welfare, MRU; Dr. O P Bhalla Foundation initiated 'CONSERVE WATER PLEDGE'.

- ✓ IQAC and Dean Student Welfare, MRU organized a one-day Workshop on Diet Nutrition and Fitness, on 20th June 2021.

- ✓ IQAC and Dean Student Welfare, MRU organized Yoga Workshop on international yoga day

- ✓ Alumni connect meetings have been organized in almost all the departments.

Chairperson then requested Dean, Research to make a presentation on Research and Innovation activities of the University for information of the Hon'ble Members.

Dean, Research and Applied Sciences, then made a detailed presentation on Research Consultancy, Innovation, Entrepreneurship & Startups initiatives which took place in recent past. The presentation included Publications, h-Index of University and Faculty Members, Research Projects submitted by the faculty members to various funding agencies, Progress of Ph.D. Scholars in last 2 years and Consultancy work carried out by faculty members.

The Dean, Research also stated that University h-index, which was 18 in 2019, has now raised to 25 in 2021. He further stated that University attained the fourth position in h-Index amongst all the Private Universities of Haryana State, which was appreciated and applauded by the Members. The Board also took note of this fact that some of the faculty members, h-Index ranges between10 to 23 and applauded the contribution of the faculties in Research work. It was advised to take up consultancy project in the area of Peace and Sustainability, Education, and Law. The strategic plan period was advised to reduce from 5 years to 2 years for better monitoring the progress.

Registrar was then requested to take up the agenda for discussion. Registrar then took up the agenda items one by one for deliberations:

2. Confirmation of the Minutes of the 16th Meeting of the Board of Management

The Hon'ble Members were informed that minutes of the 16th meeting of the Board of Management was circulated to all the members vide email dated 23.03.2021. No observation/comments was received from any of the members. Board was apprised of, the items deliberated upon in the last meeting, and requested to confirm the minutes.

Decision: Board Confirmed the Minutes of last meeting.

3. Action Taken Report on the Decisions taken in the 16th Meeting of the Board of Management.

Registrar apprised the Members with the action taken report on the decisions of the last Meeting of the Board of Management and requested the Hon'ble Members to allow him to take the report on record.

Decision: Board took the Action taken report on record.

4. Matter for Information

The Board was briefed about the following activities and requested to permit the same to take on record-

(a) Starting of UG & PG admissions for the Academic Year 2021-22.
(b) Decisions taken in the 16th Meeting of the Academic Council held on 20.07.2021
(c) Faculty/ Staff who have resigned

The Board was apprised that some of the Items recommended by the Academic Council for consideration of the Board, which have been taken up as separate Agenda of this meeting.

Decision: Board of Management took the above information on record.

5. Matter for Ratification

(I) Approval of appointment of faculty made in Academic Departments

The Board was informed that the University has made recruitments of faculty members in different academic departments on the recommendation of the Selection committee chaired by the H-Vice Chancellor. Recommend candidates, who were issued offer of appointment, some of them have joined the positions. However, two candidates at S. No. 8 & 9, have yet to join. Dr. Misha Bahmani at S. No. 9 has declined to join as she has got some other offer. Details of the candidates, who were issued offer of appointment are mentioned in the table below:

MAHARACHNA UNIVERSITY Registrar FARIDABAD

NEW JOINEES AT MRU W.E.F 01.03.2021 TILL DATE				
Sr No.	**Employee Name**	**Designation**	**Department**	**Date of Joining**
1	DR. BHAWNA SINGLA	ASSISTANT PROFESSOR	MATHS	01.03.2021
2	DR. POOJA PARMAR	ASSISTANT PROFESSOR	EDUCATION	22.04.2021
3	GARIMA CHAWLA	ASSISTANT PROFESSOR	LAW	12.07.2021
4	SAMPRITI PHUKAN	ASSISTANT PROFESSOR	LAW	19.07.2021
5	SIMRAN SINGH	ASSISTANT PROFESSOR	LAW	20.07.2021
6	CHANDNI MAGOO	ASSISTANT PROFESSOR	CST	15.07.2021
7	DR. PANKAJ MEHROTRA	ASSISTANT PROFESSOR	EDUCATION	28.07.2021
8	DR. SHAHARYAR ASAF KHAN	ASSOCIATE PROFESSOR	LAW	16.08.2021
9	DR. MISHA BAHMANI	ASSISTANT PROFESSOR	LAW	02.08.2021

The Selection proceeding was tabled in the meeting for perusal. It was ratified.

Decision: Board ratified the decision of the University.

6. Approval of intake of the existing UG / PG Programs during the Academic Session 2021-22.

The Board was apprised that the University has started admissions for UG/PG programs for the academic session 2021-22 with intake, eligibility and merit criteria as approved by BoM and GB for them last year. For the benefit of members a brief was presented by the Registrar. It was also apprised that Academic Council has ratified the same for further consideration of the Board. The Board considered and approved the Intake as under:

S. No	Name of the Program	Intake
	Bachelor of Technology	
1	B. Tech Computer Science & Engineering & Specializations	240
2	B. Tech Electronics & Communication Engineering and Specializations	30
3	B. Tech in Mechanical Engineering	60
		330
	Bachelor of Technology (Lateral Entry)	
4	B. Tech. CSE & Specilizations	24*
5	B. Tech Electronics & Communication Engineering	3*
6	B. Tech Mechanical Engineering and specializations	6*
		33

Master of Technology		
7	M. Tech. Computer Engineering	6
8	M. Tech. Electronics & Communication Engineering and specializations	6
9	M. Tech Mechanical Engineering	6
		18
Faculty of Management & Commerce		
1	BBA with Specializations	120
		120
Faculty of Applied Sciences		
1	B.Sc. (Hons.) Chemistry	15
2	B.Sc. (Hons.) Mathematics	15
3	B.Sc. (Hons.) Physics	15
4	M.Sc. Chemistry	10
5	M.Sc. Mathematics	10
6	M.Sc. Physics	10
		75
Faculty of Education and Humanities		
1	B.Ed.	50
2	B.Ed. Special Education (Learning Disability)	10
3	B.A. /B.Sc. B.Ed. Integrated	50
		110
Faculty of Law		
1	B.A. LLB (Hons.)	60
2	BBA LLB (Hons.)	60
3	B.Com. LLB (Hons)	60
4	LL.M. (One Year)	20
5	LL.M. (Two Year)	10
		210

Decision: Board approved the Intake pertaining to UG & PG Programs for the Academic Session 2021-22.

7. Approval of format of Degree Certificate for Doctor of Philosophy (Ph.D.) and Honoris Causa (D.Sc.) awarded up to January 2021.

It was submitted for the information of the Board that during the fourth convocation held on 21-Jan-2021, University awarded Doctor of Philosophy first time to two candidate namely, Sh. Jaideep Singh & Ms.. Neha Nandal enrolled as a regular candidate for the Ph.D. Program with the University and Honoris Causa, Doctor of Science (D.Sc.), to Late Dr. Sri Kumar Banerji.

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

The format of Degree used for award of degree of Doctor of Philosophy and Honoris Doctor of Science was kept the same as was approved by the Board in its 7th Meeting for Honoris Causa, Doctor of Philosophy. The format of both the Degrees were placed before the Board for ratification.

Decision: Board considered and ratified the same.

8. Consideration of Changes in Degree format for UG, PG & Ph.D. Programs and Honoris Causa (Ph.D & D.Sc.)

The Board was informed that University has initially adopted "Manav Rachna Vidyaantriksh" Logo on the Degree Certificates, which is now proposed to be replaced with approved logo of the University in the degree formats for all the programs. Accordingly, necessary changes were made in the Degree certificates and placed before the Academic Council for consideration. On being concurred by the Academic Council, the sample of new degree formats for UG / PG & Ph.D. and Honoris Causa, were placed before the Board along with old Degree Formats for consideration.

One of the Hon'ble Member enquired that if a Candidate has completed any Program with specialization, whether his specialization would be mentioned on the degree certificate or not. After detailed discussion, it was resolved that Degree Certificates will be issued program wise in generic manner, however, in respect of programs which are offered with different specialization such as B.Tech., BBA etc. specializations will be incorporated as per the guidelines of AICTE / UGC as applicable.

Decision: Board approved the new Degree Formats for UG / PG & Ph.D. and Honoris Causa, with above suggestions. Approved Format of Degree annexed as Annexure-1.

9. Consideration of Appendix to the Chapter 10 of MRU (Academic) Regulation, 2020.

It was informed to the Board that, in order to bring uniformity in the processes and system followed by all the Departments concerning conduct of meetings of SRC & DRC and to clarify some of the clause of chapter 10 of MRU (Academic) Regulation, 2020, an Appendix to the Chapter 10 of the Regulation has been prepared. The Academic Council has considered the same and recommended for approval of the Board of Management. A copy of the same was placed before the Board for its consideration and approval. The Board was appraised that this will help in smoothening the processes which some members had reported earlier.

Decision: Board considered and approved the same. Appendix to the Chapter 10 of MRU (Academic) Regulation, 2020, is annexed as Annexure-2.

10. Introduction of 3 Year LLB Program and closing of 5 Year B.Com LLB (H) Programs from Academic Session 2022-23.

Hon'ble Members were informed that the Department of Law on the basis of recommendations of its BoS has proposed to introduce 3-Years LLB program with one section of 60 from Academic Session 2022-23. The Department is of view that having a 3-years LLB program will complement the existing 5-years integrated law programs and will be helpful. Law programs have been seeing an increasing demand gradually over the years and the students, who were

not able to make up their mind early in their career just after completing 12th class or, the candidates, who wishes to gain experience in different fields of education at UG level, before converging to Law as their career option, for such students 3-years LLB program is a good option for a rewarding professional career.

Further, Department of Law has proposed to discontinue the 5 Year B.Com LLB (H) Program from session 2022-23, as it could not attract good number of student during the last five years.

The Board was also appraised that introduction of 3 year LLB program will also require approval from the Govt. of Haryana and Bar Council of India. A proposal in this regard will be submitted to the above authorities once the Board approves the proposal.

The Board was further informed that the Academic Council has concurred with both the proposal of the dept. and Okayed with recommendation to place the same before the Board for its consideration.

Decision: Board considered and approved the proposal for onward submission to the Higher Education, Govt. of Haryana and regulatory Body.

11. Approval of MRU IT Policy Mannual-2021

Board was apprised that, to prevent threats and to build a strong IT infrastructure and considering the NAAC/NBA requirements, a draft IT Policy Mannual-2021 is prepared in consultation with IT Team of the university and tabled before the Board of Management for approval. This will help in creating appropriate IT infrastructure in the university to meet the requirements of the students. The Board was requested to approve the same.

Decision: Board considered and approved the same. IT Policy annexed as Annexure-3.

12. Consideration of Annual Report 2019-20 of the University

The Board was informed that, as per the provision under the section 42 of the Haryana Private Universities Act, 2006 and amended from time to time, Annual Report of the University shall be prepared and on being approved by the Governing Body, it shall be forwarded to concerned authorities as envisaged in the Act.

A Committee headed by the Dean Academics has now prepared the draft Annual Report which has been okayed by the Vice Chancellor for placing before the Board. The draft Annual Report of the University for the Academic Year 2019-20 was tabled in the Meeting. The Board, after going through the contents of the Annual Report, advised to take opinion of Prof. V.K. Mahna, before finalizations of the Annual Report.

Decision: Board deferred decision on Annual Report with above suggestion

13. Consideration of applicability of fee payable on migration to join another University.

The Board was informed that the MRU (Migration) Policy 2021 which comprises the provisions relating to Inter Departmental Migration for UG Programs, admission through Migration from other Universities, Migration to other Universities and Migration for Ph.D. programs was taken up for approval during the 16th meeting of BoM held on 04.03.2021. While discussing the Policy

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

in the previous meeting, it was suggested to see the policy implemented by the other state private universities in connection with fees that will be payable by the student concerned for remaining duration of the course to the University for getting NOC to migrate to the other universities. Board after detailed deliberation, approved the policy with exception in the case of Migration of a student from the University and authorized the Vice Chancellor to approve the same.

After discussion with the designated officials of other Private Universities viz GD Goenka, SRM, SGT & Rishihood University, it has been observed that they are not charging any fee for further duration from the student seeking migration. However, at the time of issuance of NOC, fee is collected only for the period for which student pursued his/her Course. Accordingly, matter was placed to Vice Chancellor but he desired to place the matter again in the Board.

Hence, keeping in view that no fee being charged by the other private Universities for giving NOC to migrate from the University to another University, it was proposed that we may also follow the same and not to charge any fee for issuing NOC to student for Migration to other University other than dues payable by him.

In view of the same, Board was requested to take a decision on applicability of fee on migration to other University. One of the Hon'ble Members was of the view that Migration should be allowed only after payment of fee for the remaining years, as (i) this seat will remain vacant for rest of the period and (ii) it will help the University in retaining the students to continue the program in the University. The Hon'ble Chairman, stated that migration certificate is no more required now, to take the admission through migration in another University and if fee for the remaining year is asked to be paid, there may be possibility that student may not pay the fee and leave the course. Further, he stated that as per the University Grants Commission (Establishment and Operation of Academic Bank of Credits in Higher Education) Regulations, 2021, a student may transfer his earned credit to another University wherever he wants to pursue the program has made it quite flexible for the students.

After detailed deliberation over the same, a view emerged to look into detail of the Academic Bank of Credits Regulations and examine whether, transfer of credit has any linkages with the administrative issues primarily financial aspects. This was and agreed and discussed in next meeting.

Decision: Board deferred the proposal with the advice to examine the administrative aspects relating to transfer of academic credits in Academic Bank of Credits in Higher Education, Regulations-2021.

14. Review of the last date of Admission in Engineering and Non Engineering Programs and Fee Refund Policy for the Academic Session 2021-22.

It was informed that in the last meeting, the Board had approved that Fee Refund Policy as notified by the Regulatory Bodies (AICTE & UGC) for professional and other programs shall be followed for the Academic year 2021-22. The UGC & AICTE have notified the Academic Calendar for the Academic Session 2021-22 and same shall be implemented.

As per academic calendar of UGC, Admission Process for Undergraduate, Postgraduate (Non Engineering Programmes) in online/ offline/ blended mode **shall be completed by September**

30, 2021 and the last date for admissions to fill up the remaining vacant seats shall be **October 31, 2021.** The classes for the first batch shall commence latest by October 01, 2021. If there is a delay in declaration of result of the qualifying examinations, Higher Education Institutions may plan and start the academic session by October 18, 2021. The teaching-learning process may continue in offline/ online/ blended mode.

Further, In view of the financial hardships being faced by parents due to lockdowns and related factors, a **full refund of fees should be made on account of all cancellations** of admissions/ migrations of students **up to October 31, 2021** for the academic session 2021-2022 as a special case. The guidelines make it clear that the entire fee, including all charges, should be refunded (i.e. there should be zero cancellation charges) on account of cancellations/ migrations up to October 31, 2021.

Thereafter, on cancellation/ withdrawal of admissions up to December 31, 2021, the entire fee collected from a student **should be refunded in full after deducting not more than Rs.1000/- as processing fee.**

As per academic calendar of AICTE, Admission Process for filling up vacancies in Undergraduate, Postgraduate (Professional Programmes) **shall be completed by 20.10.2021** and classes for the existing batches shall commence from 01.10.2021 and classes of first year student shall commence latest by **25.10.2021.** In such a situation, the last date for cancellation of seats for **technical courses** with **full fee refund shall be 15.10.2021.**

As far as, MRU is concerned, the last date of admission for both Professional and Other programs is fixed as **30.09.2021**. The classes for the existing batch (Engineering & Non Engineering) have already started from 19.07.2021 & 26.07.2021 respectively. As far as first semester is concerned, the orientation for first semester shall commence from **23.08.2021.**

In view of the above decision is required to be taken on the following:

Professional Programs:

Whether or not to continue admissions for professional programs (UG & PG) upto October 20, 2021 as laid down by the AICTE in their Academic Calendar and allow full refund on cancellation till 15.10.2021.

Other Programs:

Whether or not to continue admissions in other programs (UG & PG) upto October 31, 2021 to fill up vacancies as laid down by the UGC in their Academic Calendar and allow full refund with zero cancellation changes on cancellation of admission till October 31, 2021. Thereafter, on cancellation/ withdrawal of admissions up to December 31, 2021, the entire fee collected from a student should be refunded in full after deducting not more than Rs.1000/- as processing fee.

Some of the members were of the view that classes of the University shall be commencing before the date of commencement of classes as notified by the Statutory Bodies, hence, to comply with norms will be difficult. It is advised to align the Academic Calendar of the University with the one prescribed by the AICTE and UGC for professional and non professional courses and accordingly device the admission fee refund policy of the University. Registrar, informed that the present fee refund policy notified by the regulatory Bodies are not connected with the

commencement of classes rather it is linked with last date of admission. As, in our case last date of admission is 30.09.2021, the University may not deduct any processing fee till last date of admission i.e. 30.09.2021 even if we align with the above Fee refund Policy notified by the two Regulatory Bodies. However, if university decides that no admission will be made further after 30.09.2021, the refund policy may be reviewed and decide a fresh.

Decision: Board deferred the proposal with advice to align the fee refund policy for the academic session 2021-22 and authorized Vice Chancellor to approve the same.

15. Introduction of 4.5 Year BBA-MBA Program in Peace and Sustainability Management

It was informed to the Board that the Department of Management & Commerce proposed to offer **4.5 Year Duration, BBA-MBA Program in Peace and Sustainability Management** in association with MR-Centre for Peace and Sustainability with intake 30 from the Academic Session 2022-23. The purpose to introduce this program was briefed by the Dean, Management & Commerce who stated that the program will offer to inculcate attitude of Peace & Sustainability in the field of Technology, Business, Governance, Education and Society.
The Program is proposed to be offered with intake 30 and shall have multiple Exit Options as per the policy of the NEP-2020. The student shall have the option/choice to exist from the program at any stage. In case a student leaves the program, the Course Certificate will be awarded after completion of One year, Diploma after completion of 2 Years, Bachelor Degree after Completion of 3 Year and Master's Degree after completion of the complete duration of the Program.

The proposal was placed before the Academic Council in its 16th Meeting for its consideration. The council after detailed deliberation, the Members of the Academic Council suggested that duration of the program should be rechecked as Master Degree is awarded after 5 years after 10+2. Accordingly, we have tried to check the rule laid down by the UGC for award of Master Degree and it is found that as per the Clause 8.1 of the UGC (Minimum Standards of Instruction for the Grant of the Master's Degree through Formal Education) Regulations, 2003, ***"no student shall be eligible for the award of the Master's degree unless he/she has successfully completed a minimum of two years after the First degree OR five years after Plus Two OR earned the minimum number of credits prescribed by the university for the programme".***

From the above it is evident that the Master's Degree be awarded after 5 years of +2 but as per the third option of the provision i.e. ***earned the minimum number of credits prescribed by the university for the programme"*** the University can define the duration of the program even less than Five year subject to fulfilment of Credit required for UG/PG Program.

As per the information provided by the Department, 140 Credit has been prescribed for award of BBA Degree and 60-70 Credits are required for Masters, thus to offer the above program in lesser duration of four and half, minimum 200-210 Credit will be required to be completed by the student concerned within the prescribed duration of the program considering this duration of the program has been proposed to be kept 4.5 Years for this integrated program.

After detailed deliberation on the proposal, the Board observed that "Peace and Sustainability" is not much common/prevalent today and therefore, offering such program at undergraduate level may not attract the good number of students. It would be appropriate that Centre of Peace and sustainability should offer certificate courses of different durations in peace and sustainability and the department of management offer integrated MBA program. It would be a beginning for

the Dept. of Mgt. towards PG program. Further the Department considering the introduction of BBA in Business Analytics which has received good response from the candidates though, it is introduced for the first time this year may start MBA in Business Analytics from next year. This was unanimously agreed by all the Hon'ble members and approved.

Decision: 1. Board approved that the Department of Mgt. & Commerce could go ahead with introducing integrated MBA program of 4& ½ year duration from the Academic year 2022-23. Department may also think of introducing MBA in Business Analytics from the year 2022-23.

2. Centre of Peace and Sustainability may offer certificate courses of six Months to one year duration in peace and sustainability separately.

16. Consideration and approval of faculty positions for the academic year 2021-22

Board was apprised about the number of faculty requirements, prepared by the Dean Academics for the Departments as per the programs offered by them during the academic year 2021-22. The detailed faculty requirement cadre wise & departments wise mentioned in the table was presented for consideration:

S. No.	Faculty / Academic Unit		Professor	Associate Professor	Assistant Professor	Total
1	Faculty of Engineering	Department of Computer Science and Technology	8	6	24	38
2		Department of Electronic and Communications	2	2	5	9
3		Department of Mechanical Engineering	2	2	7	11
4	Faculty of Applied Sciences	Department of Mathematics	1	3	9	13
5		Department of Physics	2	2	4	8
6		Department of Chemistry	5	1	8	14
7	Faculty of Management and Commerce	Department of Management and Commerce	1	6	4	11
8	Faculty of Law		2	4	19	25
9	Faculty of Education	Department of Education	1	5	13	19
10		Department of Humanities	0	2	0	2
	Total Faculty Sanctioned Post		150			

The proposed requirement of department wise teaching posts as presented above was deliberated and approved by the BoM.

Decision: Board approved the faculty position required for the academic year 2021-22.

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

The meeting ended with vote of thanks to the Chair.

(Dr. K. Singh)
Registrar /Member Secretary

F.NO. MRU / BoM (A&M) /Vol. IV / 2017 **Dated: 16.08.2021**

To,

1. PS to Chancellor for kind information of the Hon'ble Chancellor
2. PS to VC for kind information of the Hon'ble Vice Chancellor
3. Additional Chief Secretary to Government, Haryana Higher Edu Department, Room No. 403, 4th Floor, Mini Secretariat, Sector-17, Chandigarh.
4. PS to VP for kind information of the Hon'ble Vice President, MREI
5. Dr. M.M. Kathuria, Trustee, NIT Faridabad
6. Ms. Shalini Tuli, Associate Professor, (Nominee of the Govt)., Govt. College, Sector 16, Fbd.
7. Dr. V.K. Mahna, Ex-PVC, MRU
8. Sh. Rajiv Kapoor, ED & Group HR, Head, Uno Minda
9. Sh. Navdeep Chawla, Chairman / Managing Director, Psychotropic India Ltd. 214- 216, Sector-15, Faridabad
10. Prof. Sangeeta Banga, Dean (Academics)
11. Prof. Pradeep Varshney, Dean Research
12. Prof. Shruti Vashisht, Dean SW & HoD, ECE
13. Prof. Parul Jhajaria, Dean, Faculty of Management & Humanities (Special Invitee)
14. Prof. Versha Vahini, Associate Dean & HoD, Dept. of Law
15. Dr. Jyoti Pruthi, Associate HoD, Dept. of CST

MANAV RACHNA
Vidyanatariksha

MANAV RACHNA UNIVERSITY

Declared as State Private University vide Haryana Act 26 of 2014

With full honour confers upon

Shri Harvind Kumar Batra

The Degree of

Doctor of Philosophy (Ph.D.)

Honoris Causa

With all its rights and privileges, in witness whereof
the seal of the University is hereunto affixed
Given on this 21st day of January, 2021

(Given under the seal of the University)

कुलपति
Vice-Chancellor

कुलाधिपति
Chancellor

कुलसचिव
Registrar

फरीदाबाद (हरियाणा, भारत),
Faridabad (Haryana, India),

MANAV RACHNA UNIVERSITY
Registrar
FARIDABAD

Prepared by _____

Checked by _____

MANAV RACHNA UNIVERSITY
MRU Campus: Sector-43, Delhi-Surajkund Road, Faridabad
E-mail: dycoe@mru.edu.in URL: www.mru.edu.in

Serial No.: 17/FMC/BBA/063

Univ Regn No.: MRUMCUN012K170234

MANAV RACHNA
vidyanatariksha

MANAV RACHNA UNIVERSITY

Declared as State Private University vide Haryana Act 26 of 2014

प्रमाणित किया जाता है कि

आकाश कानन आत्मज/आत्मजा **वेंकटेश कानन**

विद्यार्थी **फैकल्टी ऑफ़ मैनेजमेंट एंड कामर्स** को इस विश्वविद्यालय

द्वारा आयोजित तत्सम्बन्धी परीक्षा उत्तीर्ण कर लेने के उपरान्त

बैचलर ऑफ़ बिज़नस एडमिनिस्ट्रेशन (एंटरप्रेन्योरशिप फैमिली बिज़नेस)

की उपाधि प्रदान की जाती है।

उन्होनें 10–अंक परिमाण पर **6.33** का सी.जी.पी.ए. प्राप्त किया है।

श्रेणी : प्रथम

This is to certify that Akash Kannan

Son/Daughter of Venkatesh Kannan

a student of the Faculty of Management & Commerce is hereby awarded the degree of

Bachelor of Business Administration (Entrepreneurship & Family Business)

on having passed the Examination

for the said degree with

CGPA of 6.33 on 10 - point scale.

Class : First

(Given under the seal of the University)

कुलपति
Vice-Chancellor

कुलसचिव
Registrar

फरीदाबाद (हरियाणा, भारत), 15 अप्रैल, 2021
Faridabad (Haryana, India), 15 April, 2021

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

कुलाधिपति
Chancellor

Prepared by _____

Checked by _____

MANAV RACHNA UNIVERSITY
MRU Campus: Sector-43, Delhi-Surajkund Road, Faridabad
E-mail: dycoe@mru.edu.in URL: www.mru.edu.in

Serial No.: 15/FMC/PHD/0141

Univ Regn No.: MRUMCDN012K150169

MANAV RACHNA Vidyanatariksha

MANAV RACHNA UNIVERSITY

Declared as State Private University vide Haryana Act 26 of 2014

प्रमाणित किया जाता है कि

जयदीप सिंह आत्मज/आत्मजा दिवाकर सिंह

अध्येता **फैकल्टी ऑफ़ मैनेजमेंट एंड कामर्स** को

डॉक्टर ऑफ़ फिलॉसफी की उपाधि, वर्ष **2020** में प्रदान की जाती है।

शोध शीर्षक :

"ए स्टडी ऑफ एनटेसीडेंट्स ऑफ एंप्लॉयी सटिस्फैकन एंड इट्स लिंकेजस विद कस्टमर डिलाइट इन सेलेक्ट इंडियन हॉस्पिटालिटी इंडस्ट्री"

This is to certify that **Jaideep Singh**

Son/Daughter of **Diwakar Singh**

a student of the **Faculty of Management & Commerce** *is hereby awarded the degree of*

Doctor of Philosophy, *in the year* **2020**.

Thesis title:

"*A Study of Antecedents of Employee Satisfaction and its Linkages with Customer Delight in Select Indian Hospitality Industry*"

(Given under the seal of the University)

कुलपति
Vice-Chancellor

कुलाधिपति
Chancellor

कुलसचिव
Registrar

फरीदाबाद (हरियाणा, भारत), 21 जनवरी, 2021
Faridabad (Haryana, India), 21.01.2021

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

Prepared by _____

Checked by _____

MANAV RACHNA UNIVERSITY
MRU Campus: Sector-43, Delhi-Surajkund Road, Faridabad
E-mail: dycoe@mru.edu.in URL: www.mru.edu.in

MANAV RACHNA UNIVERSITY
Registrar
FARIDABAD

APPENDIX OF CHAPTER 10 OF MRU (ACADEMIC) REGULATION, 2020.

In exercise of the power conferred vide section 34 of the Haryana Private Universities Act,2006 and amended from time to time, Board of Management of the University hereby makes the following provisions as appendix which shall constitute part of the Chapter 10 (Doctor of Philosophy, Ph.D.) - MRU (ACADEMIC), Regulation, 2020.

(1) Short Title, Application and Commencement

(a) This shall be called as appendix to Chapter 10 (Doctor of Philosophy, Ph.D.) of Manav Rachna University (Academic), Regulation, 2020

(b) This shall apply to all the students enrolled in Ph.D program of the University.

(c) This shall come in force from the date of approval of the Board of Management.

(2) Definition

Words and expressions used, but not defined, in these appendix shall have the meanings assigned to them in the Act, the Statutes, Ordinances and Academic Regulations of the University.

(3) Annotation of Clauses

(i). Para 1 of Clause 9: Comprehensive Review

On successful completion of the Course work, a candidate shall be required to present his/her short synopsis to SRC, which after being satisfied, will recommend the Research Proposal of the Candidate to DRC for consideration and approval.

(ii).Clause 15: Performance Monitoring

After approval of the short synopsis by DRC, the Research progress of the candidate shall be monitored by SRC and Performance Evaluation Report of SRC shall be submitted to the DRC in its meeting for acceptance/suggestions for improvement.

Note:

- The decisions, as above, will be required to be taken in meeting of SRC/DRC by inviting all the members (Internal & External) on a specified date and time.
- The suggestions / observations made by the members during the meeting need to be duly minuted in the minutes of the meeting, monitored in the next meetings while reviewing the research progress and based on it, SRC/DRC Chairperson may write their remarks on the research progress report submitted by the candidate, as prescribed and take further action as required.
- The minutes of the meeting of the committees (SRC/DRC), shall be required to be circulated to all the members of the committee irrespective their presence for their comments /observations and kept on record by the Chairperson of the SRC /DRC.
- Chairperson DRC, shall decide whether meeting of the Committee is to be convened for a day or two consecutive days, depending upon the number of candidates, who will be presenting their progress report for evaluation by the Committee with prior approval of the Competent Authority.

(iii). Clause 16: Pre-submission Seminar

(a) Reference to publications in refereed/ indexed journals as required under above clause, the candidate should refer UGC-CARE research publications listed in **"Group-II i.e. Indexed Journal".**

(b) Any research publication under the Category **"Group-I i.e. Non Indexed Journal"** shall require prior approval of the University.

(iv). Clause 17: Long Synopsis and Thesis Evaluation

(a) **Sub Clause (iii)**

— In case, DRC, Chairperson or Members of the Committee is/are Supervisors/Co-Supervisor for Candidate(s) presenting their long synopsis then the Chairperson for the DRC will be nominated, by the Vice Chancellor on the recommendation of the Dean, Research, who will be informed by the DRC Chairperson.

— If any external expert is member of the DRC and Co-Supervisor for any candidate, who is presenting his/her long synopsis before the committee, such external expert shall be substituted with another expert member nominated by the Vice Chancellor for that particular meeting of DRC, on the recommendation of the Dean, Research, who will be informed by the DRC Chairperson.

— The above procedure will be followed in other similarly situated cases.

(b) **Sub Clause (iv) & (v) Panel of Examiners**

— SRC, shall recommend the name of 8-10 experts who are holding the positions of Professor or Scientist (Scientist-F, Scientist-G) or Industry Person equivalent to Professor, from the relevant field to the DRC for preparing a panel of examiners comprising five members as prescribed under regulation.

For Manav Rachna University
SD-
Registrar

MANAV RACHNA UNIVERSITY
Registrar
FARIDABAD

IT Policy Manual

Version 1.0

MANAV RACHNA UNIVERSITY (MRU)

Delhi – Surajkund – Badkhal Road, Sector 41
Faridabad, Haryana

Website: www.manavrachna.edu.in

Version No.	Date	Description	Author	Reviewed & Approved by
1.0	xx-xcx-xxcxcx	First copy	Central IT Cell	Registrar

Table of Contents

1 Policy

The computing resources at Manav Rachna University (MRU) support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the MRU community. As a user of these services and facilities, have access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is important for user to behave in a responsible, ethical, and legal manner.

If an individual is found to be in violation of the Acceptable Use Policy, the University will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University. Individuals are also subject to central, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and local laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at MRU.

This policy applies to all users of computing resources owned or managed by MRU. Individuals covered by the policy include (but are not limited to) MRU faculty and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals and organizations accessing network services via MRU's computing facilities.

Computing resources include all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the University Libraries and Computing and Information Services), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the University's network services.

1.1 Rights and Responsibilities

Use MRU's computing facilities and services for those activities that are consistent with the educational, research and public service mission of the University and are not "Prohibited Activities".

As a member of the University community, MRU provides use of scholarly and/or work-related tools, including access to the Library, certain computer systems, servers, software and databases, the campus telephone and voice mail systems, and the Internet. It is expected from University Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (may vary depending on whether user association/ role in the University), and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of non-electronic communication.

It is responsibility of the University Community to know the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the MRU community, each individual is expected to respect the University's good name in user electronic dealings with those outside the University.

1.2 Acceptable Use

An authorised user may use only the computers, computer accounts, and computer files for which he/she has authorization.

User may not use another individual's account, or attempt to capture or guess other users' passwords.

User are individually responsible for appropriate use of all resources assigned to user , including the computer, the network address or port, software and hardware. Therefore, user are accountable to the University for all use of such resources. As an authorized MRU user of resources, user may not enable unauthorized users to access the network by using a MRU computer or a personal computer that is connected to the MRU network. [*Please refer Network Connection Policy*]

The university is bound by its contractual and license agreements respecting certain third party resources; user are expected to comply with all such agreements when using such resources.

User should make a reasonable effort to protect user passwords and to secure resources against unauthorized use or access. User must configure hardware and software in a way that reasonably prevents unauthorized users from accessing MRU's network and computing resources.

User must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

User must comply with the policies and guidelines for any specific set of resources to which user have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

User must not use MRU computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

On MRU network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless user have been specifically authorized to do so by the MRU-IT Information Security Group.

1.3 Fair Share of Resources

Computing and Information Services, and other University departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical

advantage over others in the MRU community is explicitly forbidden.

The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

1.4 Adherence with Central, State, and Local Laws

As a member of the MRU Community, user are expected to uphold local ordinances and state and federal law. Some MRU guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of MRU's computing and network resources user must:

a) Abide by all federal, state, and local laws
b) Abide by all applicable copyright laws and licenses. MRU University has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements
c) Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement
d) Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless user have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution

See the Copyright Infringement Policy, which details the policies and procedures MRU University follows in responding to notifications of alleged copyright infringements on the University network.

1.5 Privacy and Personal Rights

All users of the university's network and computing resources are expected to respect the privacy and personal rights of others.

Do not access or copy another user's email, data, programs, or other files without the written permission of MRU's Chief Information Security Officer, who is bound to the procedures outlined at Emergency Access to Accounts and Information.

Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to university discipline as well as legal action by those who are the recipient of these actions.

While the University does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that MRU is not subject to claims of institutional misconduct.

Access to files on University-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Chief Information Security Officer in conjunction with requests and/or approvals from senior members of the University, as found in the document Emergency Access to Accounts and Information. External law enforcement agencies and MRU Public Safety may request access to files through valid subpoenas and

other legally binding requests. All such requests must be approved by the General Counsel. Information obtained in this manner can be admissible in legal proceedings or in a University hearing.

1.6 Privacy in Email

While every effort is made to insure the privacy of MRU email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user.

1.7 User Compliance and Liability

When a individual use MRU computing services, and accept any University issued computing accounts, means that individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep up-to-date on changes in the computing environment, as published, using University electronic and print publication mechanisms, and to adapt to those changes as necessary. User shall be liable to hold responsibility for any unlawful activities or communications made from his / her device and account.

2 Definitions

2.1 Acceptable Use

"Acceptable use" means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

2.2 Prohibited Activities

The activities that are not consistent with the educational, research and public service mission of the University are called "Prohibited Activities". Prohibited activities include:

a) Activities that would jeopardize the University's UGC and NAAC status
b) Use of MRU's computing services and facilities for political purposes
c) Use of MRU's computing services and facilities for personal economic gain

d) Use of MRU's computing services for any unlawful activities, racial activities, threat to nation or any individual, hoax calls, impersonation etc.

3 Network Connection Policy

The purpose of this policy is to define the standards for connecting computers, servers or other devices to the University's network to protect the MRU campus network and the ability of members of the MRU community to use it.

The standards are designed to minimize the potential exposure to MRU community from damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance.

MRU must provide a secure network for educational, research, instructional and administrative needs and services. An unsecured computer on the network allows denial of service attacks, viruses, Trojans, and other compromises to enter the university's campus network, thereby affecting many computers, as well as the network's integrity. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical MRU University internal systems. Universities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the MRU network must follow specific standards and take specific actions.

This policy applies to all members of the MRU community (faculties, employees, students etc.) or visitors who have any device connected to the MRU network, including, but not limited to, desktop computers, laptops, servers, wireless computers, mobile devices, smart-phones, specialized equipment, cameras, environmental control systems, and telephone system components. The policy also applies to anyone who has systems outside the campus network that access the campus network and resources. The policy applies to university-owned computers (including those purchased with grant funds), personally-owned or leased computers that connect to the MRU network.

3.1 Appropriate Connection Methods

Devices can be connected to campus network at appropriate connectivity points including voice/data jacks, through an approved wireless network access point, via a VPN or SSH tunnel, or through remote access mechanisms such as DSL, cable modems, and traditional modems over phone lines.

Modifications or extensions to the network can frequently cause undesired effects, including loss of connectivity. These effects are not always immediate and not always located at the site of modifications. As a result, extending or modifying the MRU network must be done within the MRU-IT published guidelines. Exceptions will be made by MRU-IT for approved personnel in departments who can demonstrate competence with managing the aforementioned hardware.

3.2 Network Registration

Users of the university network need to be required to authenticate when connecting a device to it. Users may also need to install an agent on their computers before they are allowed on the network. The role of such an agent would be to audit the computer for compliance with security standards as defined in this document.

MRU-IT maintains a database of unique machine identification, network address and owner for the purposes of contacting the owner of a computer when it is necessary. For example, MRU-IT would contact the registered owner of a computer when his or her computer has been compromised and is launching a denial of service attack or if a copyright violation notice has been issued for the IP address used by that person or found to be indulged in unlawful and mollified activities.

3.3 Responsibility for Security

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

Every computer or other device connected to the network, including a desktop computer has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer at their office). For the sake of this policy, owners and caretakers are both referred to as owners.

Owners are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to the Departmental Computing Coordinator or the Departmental Systems Administrator. Therefore, it is possible that one owner manages multiple departmental machines along with his or her own personal computer. Every owner should know who is responsible for maintaining his or her machine(s).

3.4 Security Standards

Security standards apply to all devices that are connected to MRU network through standard university ports, through wireless services, and through home and off campus connections.

Owners must ensure that all computers and other devices capable of running anti-virus/anti-malware software have MRU-licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week.

Computer owners must install the most recent security patches on the system as soon as practical or as directed by Information Security. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.

Computer owners of computers that contain MRU Restricted Information should apply extra protections. MRU-IT's Information Security Group will provide consultations on request to computer owners who would like more information on further security measures. For instance, individuals who are maintaining files with Social Security information or other sensitive personal information should take extra care in managing their equipment and securing it appropriately.

3.5 Centrally-Provided Network-Based Services

MRU-IT, the central computing organization, is responsible for providing reliable network services for the entire campus. As such, individuals or departments may not run any service which disrupts or interferes with centrally-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions will be made by MRU-IT for approved personnel in departments who can demonstrate competence with managing the aforementioned services. Also, individuals or departments may not run any service or server which requests from an individual their MRU-IT-maintained password.

3.6 Protection of the Network

MRU-IT uses multiple methods to protect the MRU network:

a) monitoring for external intruders
b) scanning hosts on the network for suspicious anomalies
c) blocking harmful traffic

All network traffic passing in or out of MRU's network is monitored by an intrusion detection system for signs of compromises. By connecting a computer or device to the network, user are acknowledging that the network traffic to and from user computer may be scanned.

MRU-IT routinely scans the MRU network, looking for vulnerabilities. At times, more extensive testing may be necessary to detect and confirm the existence of vulnerabilities. By connecting to the network, user agree to have user computer or device scanned for possible vulnerabilities.

MRU-IT reserves the right to take necessary steps to contain security exposures to the University and or improper network traffic. MRU-IT will take action to contain devices that exhibit the behaviours indicated below, and allow normal traffic and central services to resume.

a) imposing an exceptional load on a campus service
b) exhibiting a pattern of network traffic that disrupts centrally provided services
c) exhibiting a pattern of malicious network traffic associated with scanning or attacking others
d) exhibiting behaviour consistent with host compromise

MRU-IT reserves the right to restrict certain types of traffic coming into and across the MRU network. MRU-IT restricts traffic that is known to cause damage to the network or hosts on it, such as NETBIOS. MRU-IT also may control other types of traffic that consume too much network capacity, such as filesharing traffic.

By connecting to the network, it is expected that the individual has acknowledged that a computer or device that exhibits any of the behaviours listed above is in violation of this policy and will be removed from the network until it meets compliancy standards.

4 Handling of MRU Restricted Information

MRU University is dedicated to ensuring the privacy and proper handling of private and restricted information of its students, employees, and individuals associated with the University. The primary purpose of this policy is to ensure that the necessary policy and awareness exist so that University employees and students comply with all applicable laws and regulations. This document establishes minimum requirements for the proper handling and protection of MRU Restricted Information. All departments shall limit access to MRU Restricted Information to those individuals with a university and/or business need to the information in order to do their job.

This policy applies to all MRU Restricted Information, which includes but is not limited to: Personal identifications, credit card numbers, medical records, dates of birth, driver's license numbers, addresses, and passport information.

Restricted information is not meant only for university operational, business and student data. Research data also utilizes highly sensitive, confidential, restricted and regulated information. Many Data use Agreements stipulate and dictate strong security measures for the use of the data.

The restricted information is covered in any tangible format, including but are not limited to, paper, photographs, film, audio and videotapes, microforms, drawings, databases, email, and any other electronic records.

All members of the MRU community, including staff, faculty, students, affiliates, volunteers, and third party vendors or contractors shall comply with this policy. Vendor contracts should include a clause referencing this policy.

4.1 Access, Storage, Transmission & Back-up of Restricted Information Access

4.1.1 Access

Access controls to all MRU Restricted Information must be documented.
MRU Restricted Information must have a designated Data Owner who authorizes such access.

4.1.2 Storage

MRU Restricted Information in electronic format must be stored on a server centrally managed by Computing and Information Services (MRU-IT) or in an environment that is under strict legal contracts with the university that meet this policy, and not on a workstation, laptop, portable storage device, or locally managed server. Exceptions must be reviewed and approved in writing by the MRU- Chief Information Security officer.

An approved local machine must be in a physically secure location and require a unique logon with a strong password for each individual with authorized access (i.e. shared accounts and passwords are prohibited). Security logs must be enabled and periodically reviewed by the locally approved department.

MRU Restricted Information must be housed on a server or approved workstation that meets current operating system, hardware and software support levels.

MRU Restricted Information in any hard copy format must be stored in locked cabinets or offices, and not be able to be accessed by unauthorized persons.

4.1.3 Transmission

MRU Restricted Information should never be transmitted over the network "in the clear" rather it should always be transmitted using an Information Security Group-approved encryption mechanism.

MRU Restricted Information should never be transmitted via unencrypted email. Password-protected documents or spreadsheets can be used as attachments in certain cases, with approval of the Chief Information Security Officer.

4.1.4 Backups

It is the responsibility of everyone entrusted with MRU Restricted Information to back it up and store it in a secure and controlled location by themselves. Backup of MRU Restricted Information should be encrypted if technically feasible.

The backup of central server and databases will be taken on tapes on rotation basis, there should be an incremental backup to be taken every day and full back up need to be taken twice a week. The back-up data should be kept in two copies. One copy will be stored locally for any emergency restoration and other copy will be stored physically apart out of the campus premises but may be within the city.

4.2 Release of Information

Restricted information concerning individual students or employees may be released only if the release of such information has been authorized by the Data Owner (the University employee identified as being responsible for the classification and data oversight for a functional area, or certain type of protected

information). The Data Owner is responsible for the protection, confidentiality, and release of the information assigned to them, in accordance with University Policy, regulatory mandates, and legal obligations to release.

Additional information on the roles of the Data Owner can be found in the Data Protection Roles and Responsibilities Section of this document.

4.3 Confidentiality Agreement

Data Owners, who authorize access to MRU Restricted Information, should ensure that those with access sign a Confidentiality Agreement. All authorized users of MRU Restricted Information are also required to successfully complete the "Protecting MRU Information" class (contact Computing Accounts and Passwords for details).

4.4 Special Statement on the Collection, Storage, and Use of Personal Identifications

While it is recognized that a small number of areas, departments, and processes have a need to utilize personal identifications, any use of this identifier puts members of the MRU community at a greater risk of identity theft. As a result, any Department of MRU that currently uses, or wishes to collect, store, or use personal identifications in any format must:

a) Show institutional need
b) Receive approval from the Data, Privacy, and Records Management Steering Committee
c) Permit audits (including server and application security) at least annually to ensure safe SSN handling

Additional information specific to personal identifications can be found in the Personal identifications – Usage and Protection Requirements.

4.5 Special Statement on Research Data

As a research institution, MRU collects, stores and utilizes large amounts of research data which may be restricted, confidential and protected information. In addition to the stipulations on handling such information as outlined in this policy, guidance and oversight is provided by the Office of the Director of Research (ODR). ODR assists faculty in ensuring that research complies with institutional and federal standards, beginning with proposal preparation and review, and extending throughout the performance of the research and into evaluation and reporting of research project results.

4.6 Policy Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment

4.7 Computing Passwords Policy

Computing Passwords Policy describes the University's requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity

of malicious hackers and spammers, they are very often also the weakest link in securing data. Password use must therefore adhere to the policy statement found below.

This policy applies to anyone accessing or utilizing MRU network or data. This use may include, but is not limited to, the following: personal computers, laptops, MRU-issued cell phones, and hand-held factor computing devices (e.g., PDAs, USB memory keys, electronic organizers), as well as MRU electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

4.8 General Password Guidelines

All passwords (e.g., email, web, desktop computer, laptop etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

Central and departmental account managers, data trustees, and security and/or system administrators are expected to set a good example through a consistent practice of sound security procedures.

All passwords must meet the following minimum standards, except where technically infeasible:

a) be at least ten characters in length (for Brown network passwords, eight for Google mail)
b) contain at least one lowercase character
c) contain at least one number
d) contain at least one special character
e) contain at least one uppercase character
f) cannot contain user first name, last name, or username
g) cannot match user last three passwords
h) To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password
i) All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured
j) Passwords should not be inserted into email messages or other forms of electronic communication without the consent of the Information Security Group (ISG)
k) Passwords that could be used to access sensitive information must be encrypted in transit
l) The same password should not be used for access needs external to Brown (e.g., online banking, benefits, etc.)
m) It is recommended that passwords be changed at least every six months
n) Individual passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of ISG and must have

a primary responsible contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those

passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.

o) If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the Departmental Computing Co-ordinator (DCC).

p) Password cracking or guessing may be performed on a periodic or random basis by ISG or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

4.9 Account Administration Standards

In addition to the general password guidelines listed above, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

a) Passwords must be changed at least every six months

b) Where technically and administratively feasible, attempts to guess a password should be automatically limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes

c) Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the Information Security Group

4.10 Shared Accounts

In addition to the general password standards listed above, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

a) Passwords for servers must be changed as personnel changes occur

b) If an account or password is suspected to have been compromised, the incident must be reported to ISG and potentially affected passwords must be changed immediately

c) Where technically or administratively feasible, attempts to guess a password should be limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes

d) Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks

e) Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the Information Security Group

Note: Log files should never contain password information

5 Data Protection Roles & Responsibilities

There are four basic roles for proper data management and protection at MRU:

a) Data Owner

b) Manager of Policies & Procedures for access to that data

c) Manager of the infrastructure and account access

d) Data user

It is important that

- All MRU Restricted Information should have an identified owner
- Anyone who has been entrusted with sensitive information has a responsibility to the data's owner for its proper use and protection.

The following chart breaks out above roles and defines their responsibilities. The listed example is for the handling of financial business information and illustrates one combination of roles and responsibilities.

Responsible Position or Individual	**Key Responsibilities**	**Example** ***(Financial Data)***
Registrar(Chairperson)	• Data owner for their functional area, responsible for its management and participating in establishing policies. • Promotes data resource management for the good of the entire University.	University Controller
Departmental Heads	• Manage access to their functional area's data. • Provide input in policy implementation and resulting procedures • Awareness/ training for those individuals who have access to "MRU sensitive information" in the course of their jobs.	Assistant Controller
Zone Leaders	• Provide a secure infrastructure in support of the data, including, but not limited to: physical security, backup and recovery processes as well as secure transmission of the data. • Grant/ Revoke access privileges to authorized system users and maintain records. • Ensure individuals have access only to that information for which they have been authorized, and that access is removed in a timely fashion when no longer needed. • System Administrator and/or Departmental Computing Coordinators are accountable for data within their specific areas or departments. • Computing and Information Services for centrally held data.	Technical Support / System Administrator

Manager ICT	• Protecting the security and integrity of the data as detailed in the Policy on the "Handling of MRU Restricted Information" • Report weakness in the protection of data to IT Security	User of Workday Financials System

5 Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk at intercom No. 4444 or email at team-helpdesk@manavrachna.net. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

6 Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

7 Further Information

If user have any queries in relation to this policy, please contact:
General Manager IT
Email: gm.it@mrvpl.in

Hardware Acquisition, Disposition and Replacement Policy

Version 1.0

The following policy outlines MRU approach to the acquisition of information technology hardware. This policy establishes expectations for the purchase, use and re-use of technology hardware.

MANAV RACHNA UNIVERSITY (MRU)

Delhi – Surajkund – Badkhal Road, Sector 41
Faridabad, Haryana

Website: www.manavrachna.edu.in

Version No.	Date	Description	Author	Reviewed & Approved by
1.0	xx-xcx-xxcxcx	First copy	Central IT Cell	Registrar

Table of Contents

1 Policy

The University has entrusted IT Department with responsibility for the support and timely maintenance of the University network, servers and workstations to include University owned computer hardware, software and peripherals. This policy establishes expectations for the purchase, use and re-use of technology hardware that assures, as a community, as responsibilities towards the University resources, aware of security considerations and consistent in MRU practices.

2 Definitions

2.1 Technology

"Technology" means a cable or small digital camera to a desktop computer/ laptop or printer. Throughout this policy the word "technology" when not otherwise qualified refers only to computers, monitors, tablets, printers and most devices that connect to the University's network. While IT department will gladly offer advice and guidance and/or facilitate making other types of purchases, this policy is not aimed at those needing small peripherals (for example cables, an adaptor, a specialized mouse, a thumb drive, a small webcam, a voice recorder, microphone or speaker.)

2.2 University-Owned

A "University-owned" computer is defined as a computer that is optimally configured for the general activities associated with being a staff or faculty member and optimized to work on the MRU network with associated adequate security provisions. This may be new or used equipment depending on circumstances.

3 Technology Equipment Purchasing

To achieve the best possible and most effective service levels for all MRU-owned technology, technology hardware purchases are made under the suggestion of IT department through central procurement department.

By working through IT department, faculty and staff can expect assistance and guidance that helps to assure purchases are sustainable, compatible with existing systems, and can be adequately supported. To aid in this endeavour, IT department in association with the central procurement department has negotiated purchasing agreements with hardware, software, network, and telecommunication vendors, service agencies, multimedia companies, software developers, and others. Involving IT department in technology purchases and taking advantage of pre-negotiated purchasing agreements helps assure the needs of our campus users are met, such as:

a) Compatibility with MRU network environment.
b) Compliance with MRU security requirements and policies.
c) Suitability, based on needs assessment.

d) Licensing compliance for any bundled software purchases that accompany hardware devices.
e) Hardware that can be efficiently supported.
f) All equipment is entered into the University's asset management system

Standardizing equipment purchased allows the MRU to efficiently select and manage technology, obtain better technology pricing, reduce maintenance costs and increase access to training and assistance. These standards are re-evaluated periodically based on common needs, vendor offerings, cost, reliability, supportability, quality, sustainability, compliance with recycling policies and timeliness of vendor response.

4 Computers for Active Faculty & Professional Staff

Standard technology purchases are part of MRU Annual computer replacement cycle which focuses on the primary computer provided to active faculty and staff.

a) Manav Rachna University (MRU)will provide one "University-owned" computer to each member of the faculty and professional staff of the University, including visiting faculty for official use.
b) In case, a faculty member requests for a primary computer above the standard configuration, the requests are typically reviewed by the IT Core Committee. If approved, the faculty member may have to use his or her department, grant or endowed fund to cover the additional cost. It is not allowable for an individual's to use their own personal resources to pay for this cost differential.
c) Computers and equipment should be returned to IT TRC (Technical Repairing Centre) at the end of their useful life and are not automatically eligible for replacement. Depending on age and condition, IT TRC may use for parts, properly remove data and/or recycle retired equipment. "Beyond the end of its useful life" is generally defined by IT TRC as equipment that is: broken, unable to run a newer operating system, requires an operating system that is considered end of life, or lacks necessary storage or memory to apply critical security patches, browser or software updates.
d) Computer purchases cannot be made for individual's personal use. IT department will, from time to time, make information available from some vendors that offer special incentives to employees for their personal use but those transactions are carried out directly between the vendor and the employee.
e) Departmental computer purchases may not be charged to an individual's University provided purchase card or reimbursed through an expense voucher. MRU will not reimburse nor support the purchase of any technology-related item, unless that purchase was made through and/or with the knowledge and approval of IT and core committee..
f) Should an individual's position require more than 1 computer, the individual's department bears the cost of the additional equipment from their allotted annual budget. That additional equipment will be given to IT Help Desk when it is no longer needed, or when it reaches the end of its useful life. IT staff will work with departments to determine whether equipment is no longer needed.
g) Additional desktop or laptop computers or desired peripherals such as docking stations or external monitors for laptops (either for individuals or to share within a department) are

purchased through central procurement department, but charged to departmental annual budget.

h) Because of data security concerns, administrative departments are strongly discouraged from purchasing extra shared equipment for their department (for example a shared travel laptop that is only periodically used.)

i) The majority of faculty and staff have their primary computer issued by IT department. There are a few exceptions to this. Despite this exception for primary issuance source, all other policies remain in effect.

5 Ownership and Sale of University-purchased equipment

All technology equipment, regardless of how the purchase was originally funded (departmental funds, IT funds, endowed funds, etc.) remains the property of Manav Rachna University. MRU does not consider requests for sale or retaining for non- University uses of equipment to faculty, staff, retirees or students; for example at the time of departure from MRU. This is true regardless of how the equipment purchase was originally funded. For a variety of reasons including information security, restrictions of software licensing contracts and general interest of fairness to all who might want to buy used goods from the University, IT department is not authorized to sell or give away equipment directly to individuals._Other questions about purchase or sale of University equipment should be directed to the University IT Core Committee.

6 Management of Computer Replacement/Upgrades

6.1 Hardware Replacement Policy

University-owned individual-use computers are "generally" replaced every five years. This is done for several reasons, like:

- to provide community members with the current operating systems and sufficient power for the latest software applications
- to protect our campus network by updating the security protections that come with more recent operating systems
- to maintain a reasonable number of hardware configurations that can be well supported by limited staff

IT department will engage in an **Annual** replacement plan by examining existing inventory of all University-owned hardware, making an initial recommendation for replacement based on the needs of various faculty and staff members and the funds that are available for hardware replacement. The **Department Chairs or Administrative Department** heads will then review these recommendations to make the necessary adjustments to arrive at the final plan. Depending on the adjustments made, allocations of hardware are likely to be changed, particularly if there are funding constraints within the department.

Individuals will be notified prior to the replacement of their computer and will be given an option to request delaying their replacement by no more than one year. This extension will be granted if

the computer meets the needs of the individual for another year, and if the operating system and other software will be supported for another year.
The plan will take into consideration the budget constraints and the academic cycles of various academic and administrative departments to schedule the purchase and replacement of hardware. IT staff will contact the **Chairs or the Administrative department heads** in advance of replacement for consultation, scheduling and training.

IT Staff will assist users in the transfer of data from the old computer to the new one. IT Staff will also assist in the installation of any custom applications that the user needs. However, IT Staff cannot assist in transferring any custom applications that are not supported by the University that the user had installed on their own on the older computer. In many cases, these installations will require original CDs or DVDs and serial numbers for which the user is responsible. Therefore, any reinstallation of these applications is the responsibility of the user. After the data has been transferred to the new computer and the user confirms that everything has been transferred correctly, IT staff will remove the older hardware usually within a day or two.

IT Help Desk maintains customized software images for the following standard configurations:

- Thin Clients - Appropriate for administrative staff that use the computer for basic use such as email, Office applications, basic Banner access and the web.
- Intermediate Windows Desktop Computer - This will be the standard computer for faculty who want a Windows desktop computer. This is also appropriate for an administrative user
- Windows Laptop - Ideal for anyone who travels a lot, and for use in both office and home.

In addition, IT Help Desk will recommend advanced, custom configurations for Windows PC Desktop, Windows PC Laptop, If requested. If a faculty or staff member eligible for replacement needs an advanced configuration, the same shall be routed through their HoDs to IT department for further actions.

6.1.1 Newly-hired Faculty

Each new tenure-track faculty member will be provided with a standard desktop or laptop Windows or Mac computer at the beginning of their first year depending on his requirements as decided by the department head.

6.1.2 Current Faculty

All tenured professors of the practice and lecturers on continuing appointments are eligible for an appropriate Windows notebook or desktop computer when their existing computers are due for replacement.

6.1.3 Part-time Faculty

Faculty working part-time are eligible for a desktop computer only

6.1.4 Shared Computers

There are many offices that require additional computers for their student employees, temporary employees, or teaching assistants. IT Help Desk will assess the need in these areas and provide the minimum number of shared computers. IT department will manage these requests by recommendations purchasing some of the base desktop configurations as well as use some of the computers that are being replaced for this purpose. In the long run, we will use Thin Clients for this purpose, resulting in a far more functional and cost effective solution.

6.2 Policy for Loss and Damage of Equipment

6.2.1 Damage to Equipment

Faculty & Staff who receives a University owned computing device (such as a computer or laptop) are expected to return it to University at the end of its life cycle. In the event a computer is damaged, the individual or department will be responsible for the repair or replacement of the computer. In these cases, IT TRC will provide the most cost-effective solution taking into consideration factors such as the age of the computer and the extent of the damage.

6.2.2 Loss of Equipment

If the equipment is lost on University property, it should be reported to the Campus security and Police immediately and IT Help Desk will find an appropriate replacement computer for the faculty or staff who lost the computer. If the equipment (such as a laptop or tablet) is lost outside the University property, then the individual or department is responsible for the cost of replacing the equipment with an appropriate device.

6.3 Disposition of Replaced Equipment

When a new computer is delivered by IT, and the recipient has worked with the delivering technician to assure it is working satisfactorily, the old computer will be returned to IT. IT can typically derive several years of service from a computer beyond its first years as a faculty/staff primary workstation, thereby optimizing the lifetime service an individual computer can provide to the campus. IT will gladly pick up other unused older computer equipment that was previously purchased by the University. This equipment may be repurposed on campus, responsibly recycled, or donated to worthy local and international causes after being cleaned of data and software.

6.3.1 Computer return at time of departure

When an employee departs, IT is typically alerted several weeks in advance by weekly automated reports provided by Human Resources and will arrange to pick up the departing employee's computing equipment when they depart. If a device needs to be reassigned to a different user, even within the same department, IT must retrieve the device, scrub it of data, update the University's asset database and deliver it to the new user.

6.3.2 Data retention when employees depart

For liability reasons, it is considered bad business practice to allow a department to retain a departing colleague's computer in order to retain or retrieve files for departmental operations. Under normal departing circumstances, a department should work with their colleague to relocate files from an employee's computer to an accessible and shared location prior to their last day of work. IT Staff is happy to advise and assist. In circumstances where an employee departs suddenly or unexpectedly, IT Staff will work with colleagues in that department to retrieve and retain relevant files before removing the computer. Departments are urged to establish operating

practices that avoid creating and maintaining critical operational files on an individual employee office computer.

7 Asset Management

IT Help Desk will affix MRU asset tag (typically a small sticker with a unique number on it) on each asset subject to this policy and will maintain an inventory database with I T Manager to include a description of the device and who it is assigned to, and how it was paid for if it was funded outside of IT Department.

IT Help Desk may install software to track information about the device, which is essential for locating equipment when it is lost or stolen; and in some cases being able to reliably remove data from a stolen asset. IT may also periodically conduct a physical inventory to ensure asset records align with the physical location and individual we believe has possession of them. IT may also work with departments to retrieve and re-distribute equipment that is not being utilized.

8 Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

9 Further Information

If user have any queries in relation to this policy, please contact:
Director of IT Services

MANAV RACHNA UNIVERSITY (MRU)

Delhi – Surajkund – Badkhal Road, Sector 41 Faridabad, Haryana

Website: www.manavrachna.edu.in

E-WASTE MANAGEMENT POLICY

Introduction:

Manav Rachna University, established by an 'Act' (No. 30) of 2008 of the Government of Haryana, and approved by the University Grants Commission (UGC), since inception in 2008. The University is located on Delhi Surajkund Badkhal Road. The University stands committed to the ideals of Late Dr. O P Bhalla – Right Philosophy, Right Knowledge, and Right Conduct – in branches of the knowledge tree a cloud of knowledge activity (Vidyanatariksha) and aspires to be recognized as the ultimate destination for world-class education.

After the University was established in 2002, Dental, Engineering, Management, Law, Sciences, Physiotherapy, Hotel Management, Graphical Design, Architecture, Journalism, Fine Arts, Language Studies, have been established to meet rising aspirations of the use. The campus is laid out with picturesque landscape, numerous buildings of various designs and wide road network. It presents a spectacle of harmony in architecture and natural beauty. The University is equipped with all modern facilities such as road networks, water supply, street lighting, electricity supply and parks/ lawns including Purified drinking water and highly efficient effluent / sewage treatment system.

With expansion, over a period of time and growing ICT demands, the need was felt of a systematized E-waste management system.

Definition of E-waste:

Electronic waste (e-waste) means waste electrical and electronic equipment whole or in-part or rejects from their manufacturing and repair process, which are intended to be discarded.

Steps followed by the University to dispose-off E-waste:

- The University awards the contract for Electrical/Electronic goods recycling and disposal to the govt. authorised vendor selected by the IT committee.
- All University departments/colleges/branches will take consideration of the disposal/obsolete/condemnation policy of information technology policy of (Uttar Pradesh region

Category	Nature	Items	Useful/productive life
1	Immediate obsolescence/use and throw products	Printing consumables(ink toners),floppies, CDs, DVDs, Digital Audio Tapes(DAT), UPS Batteries	As per usage. No. residual value determined. However, proper inventories of purchase, issue and final use/disposal etc. would be maintained in order to keep an accounting system.
II	Low life/Fast obsolescence products	Mobile phones	Two years
		Laptops, pen drive, External Hard Disk Drive(HDD) etc.	Three years in case of Laptops, pen Drive, HDD etc. For replacement, residual values determined separately
III	Medium obsolescence/ medium life products	Desktops, printers, multifunctional devices, scanners, multimedia projectors, UPS system etc.	Five years for replacement
IV	Slow obsolescence/long life products	Fax, cameras, TVs, DVD players, etc.	Seven years

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

V	Software	Software like MS office, Oracle, MS-SQL,MS-windows, Antivirus etc.	Please refer to the explanation given in (software) policy
Note:	The above mentioned items can be used beyond the mentioned/specified life till such time these items continue to serve the purpose.		
	Before obsoleting / disposal / condemnation of equipment, all university colleges / departments / branches will consider the following steps.		

- The following equipment will be considered for obsoleting/disposal/ condemnation

The equipment will be covered under electronic e - waste equipment like TV, air conditioners and information technology/ telecommunication equipment like centralized data processor mainframe, servers, minicomputers, personal computer, notebook, printer, cartridge, scanner, multifunctional printer, electrical and electronic typewriter, user terminal and system, FAX, telephone, cordless phone, UPS batteries, UPS, Stabilizers, DVD players, CVTs, DVD, CD, Floppies, pen drive, internal and external
HDD, RAM, LCD & DLP projector, Head phones, computer speakers, computer MIC, VGA cable, data cable, networking items like Switch, hub, router, Modems, LAN card and other electronics cards like sound, graphics, PCI cards etc.

E-WASTE DISPOSAL SOP

1. University will send its details of all e-waste equipment through IT department in association with central purchase committee
2. All obsolete / condemned material will be verified / inspected by the inspection committee. Inspection committee will work up to the completion of first phase inspection of equipment under consideration of obsolete/ disposed / condemned e-waste material.
3. In initial stage, all the departments will condemn / write-off their electronic / electrical items in the following steps.
   a. They will submit the details of the items as shown below to the IT department.

S#	Item description	Date of purchase or year of purchase	Stock register page No.	Qty	Unit price	Total price	Purchase details	Status(working or not working)

   b. The colleges / departments /branches will submit it to the IT department. The lists prepared and duly signed within ten days from the date of letter issued by the respective college / department

MANAV RACHNA UNIVERSITY Registrar FARIDABAD

c. Further, a letter will be issued by the IT department with the date and time of visit of inspection committee to inspect / verify the equipment of all concerned college / departments / branches as submitted in their obsolete / disposed / condemned equipment list.
d. All obsolete / disposed / condemned equipment and stock register will be presented and shown by all colleges / departments /branches to the inspection committee during the time of the inspection visit
e. Inspection committee will verify the condition of all equipment as submitted by the colleges / departments /branches on the site.

4. After approval from the competent authority, IT department MRU will send the University consolidated list of obsolete / disposed / condemned material to the vendor and obtain govt certificate for authorised disposal of the goods.
5. All colleges / departments / branches will retain this obsolete / disposed / condemned material at their site and it will be picked by the e-waste vendor.

NOTE: This E – Waste management system will be implemented on disposition of replaced equipment under Hardware Acquisition, Disposition and Replacement Policy.

Software Licensing Policy

Version 1.0

This policy is to address the use of computer software in the Manav Rachna University and to establish guidelines of responsibility. The purpose of this document is to define a consistent practice for the purchase and distribution of software within the University.

MANAV RACHNA UNIVERSITY (MRU)

Delhi – Surajkund – Badkhal Road, Sector 41
Faridabad, Haryana

Website: www.manavrachna.edu.in

Version No.	Date	Description	Author	Reviewed & Approved by
1.0	xx-xcx-xxcxcx	First copy	Central IT Cell	Registrar

Table of Contents

1 Policy

1.1 Software Licensing Compliance

The scope of this Policy on Software Licensing applies to the following:

a) University staff , faculties and students those who are in use of university or individual computers, laptops, tabs or any other IT related devices.
b) Software on workstations (e.g. PCs and laptops) as well as servers.
c) Software on workstations in either of the following categories:
    i. Workstations which belong to the University.
    ii. Workstations which are privately owned, but which are being used for University business and supported by the University.

a) The University has a responsibility to ensure that all software used by members of the University using hardware supplied or supported by the University, is appropriately licensed.
b) Individual users of software applications have a responsibility to ensure that:
    i. Software installed on workstations for which they have some responsibility is licensed.
    ii. The software is either named on the list of University/College list of approved and supported software, or otherwise use of the software has been agreed with/notified to the College IT department.
    iii. The software is not named on the list of prohibited software maintained at the University/College level.
    iv. They are complying with the conditions of use of respective licenses

c) A central list of supported software approved for use within the University will be maintained by IT Services and College IT Managers, as well as a list of specifically prohibited software (e.g. on security grounds or inappropriate use of University resources). Use of software which may not require a license, e.g. Freeware or Shareware, may only be used if it is on the list of officially approved software. Usage of approved screensavers will be specified at the College level.

    i. Each user must take responsibility for their own particular use of software, in accordance with the license terms and End User License Agreement.
    ii. The University's Conditions of Use of Computing and Network Facilities contains the following stipulations concerning use of licensed software – failure to comply with these could constitute a disciplinary offence:

        a. The University reserves the right for access to be granted to computer audit staff without notice to enable them to check against an inventory of licensed

software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by such audit staff and reported

b. to the
Director of IT / committee, who may initiate disciplinary proceedings."

c. Where software has been electronically downloaded from IT Services computer systems requiring user authentication by means of a username and password, the user must read and comply with the licensing conditions for that software, and the act of downloading indicates acceptance of the licensing conditions pertinent to that software.

d. All persons who are licensed to use software or who control access to any computing and/or network resources are obliged to take all reasonable care to prevent the illicit copying and use of software and documentation.

e. No one shall introduce on to computer systems any software or other material requiring a license for which a valid license is not in place.

1.2 Software Inventories

a) A software inventory must be set up and centrally maintained at the University/College level, with responsibility for this taken by the IT Manager, and similarly a nominated IT Services manager being responsible for the software inventory within Corporate Services. The format should be as close as possible to the University standard format specified by IT department.

b) This software inventory will be used to match the number of software licenses purchased against the number of staff licenses in use; also to check that the software licenses are current, i.e. have not expired. This monitoring must be carried out on a regular basis, and licenses purchased appropriately if required to rectify any discrepancies identified.

c) The inventory must take account of staff leavers, i.e. identifying software licenses that are no longer being used. Unused software licenses remain the responsibility of the College IT Manager. Any transfer of such licenses between Colleges should be recorded within the inventory.

d) The same Managers/Staff responsible for the software inventory are also responsible for maintaining copies of the software licenses relating to the inventory.

e) Use of Freeware/Shareware software should also be monitored in order to ascertain firstly that use of the software is actually free for use for business use within the University, and secondly that the use of such Freeware/Shareware does not pose any security risks. Beyond carrying out these checks, it is not necessary to either record the usage of such software, or maintain copies of software licenses.

1.3 Software Purchasing

a) Software purchasing must be limited just to IT staff themselves or in association with central purchase department, together with any other nominated individuals authorized by the College Management. A list of such additional authorized individuals must be documented and maintained by the College IT Manager.

b) These authorized members of staff must also sign off individual software purchases.

1.4 Storage of Software Media and Licenses

a) Software and media must be stored in a suitably secure and accessible location, and take into account the Business Continuity requirements, including for the case of loss of a server, or even potential loss of a building.
b) The location of the software media should be recorded on the software inventory, preferably in software library.
c) Similar consideration must be given to software which has been electronically downloaded, and it should be stored on an appropriate server. A hard copy of the licence or certificate should also be stored.

1.5 Authorized Installation of Software

a) Only authorized IT Staff within IT Services or University/College IT support staff are permitted to undertake installation of software. Other non-IT staff will be permitted to undertake installation of software only if authorized on the exception list maintained by the University/College IT department (or equivalent).
b) The same IT installation staff (or other staff specifically authorized to install software) are also responsible for ensuring that the software which they are installing is appropriately licensed and recorded in the relevant software inventory.

1.6 Software Audit and Use of Audit Tools

a) Wherever possible, access to the use of software by individuals should be controlled by Active Directory, thereby enabling both potentially automatic distribution of software applications, as well as automated use of audit tools
b) Support staff, either in IT services centrally, or within Colleges, have the responsibility for using these automated audit tools to ensure compliance by the University, i.e. confirmation that the number of licenses held corresponds with the actual number of users of the software as specified by the license conditions
c) An exception list of those devices which are excluded from such an audit must be specified at the College level, e.g. laptops and devices on the wireless network.
d) All University workstations and servers must have the standard corporate tools installed on them as part of their build to enable the software monitoring to take place. Any exception to this must be authorized and documented at the College level.
e) If suitable automated tracking software is available, support staff should use this in order to identify any software which may no longer be required within the University, with a view to either re-utilizing such software, or arranging for its disposal if redundant.

1.7 Disposal of Software

When permanently disposing of equipment containing storage media, all licensed software must be irretrievably deleted either before the equipment is moved off-site, or by utilizing an approved 3rd party off-site service.

2 Role and Responsibilities

2.1 College IT Help Desk

Responsibilities of the College IT HELP DESK in respect of software licensing staff can be summarized as follows:

a) Maintaining a University/College list of approved/supported software.
b) Maintaining a University/College list of prohibited software.
c) Maintaining a software inventory for the College (or Corporate Services).
d) Maintaining copies of the software licenses relating to the inventory.
e) Ensuring that IT support staff carries out a regular automated audit of software in use on workstations.

2.2 IT Services Staff Authorized to Install Software

Responsibilities of IT Services staff authorized to install software in respect of software licensing can be summarized as follows:

a) Ensuring, with the user, that software being used on the workstation is licensed, and approved/not prohibited.
b) Ensuring, with the user, that they are complying with the conditions of the software license. Ensuring that the installed software is recorded in the software inventory.

2.3 University Staff Using Workstations

Responsibilities of University staff using workstations in respect of software Licensing can be summarized as follows:

a) Ensuring that software being used on the workstation is licensed, and approved/not prohibited.
b) Ensuring that they are complying with the conditions of the software license.
c) Disposing of redundant software appropriately

3 Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk or respective zone leaders On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

4 Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

5 Further Information

If user have any queries in relation to this policy, please contact:
General Manager of IT Services

Data Management Policy

Version 1.0

This Data Management Policy is designed to help the MRU University understand their responsibilities with regards to the protection of electronic data. In particular electronic data and information belonging to, held or used by, MRU University.

MANAV RACHNA UNIVERSITY (MRU)

Delhi – Surajkund – Badkhal Road, Sector 41
Faridabad, Haryana

Website: www.manavrachna.edu.in

Version No.	Date	Description	Author	Reviewed & Approved by
1.0	xx-xcx-xxcxcx	First copy	Central IT Cell	Registrar

MANAV RACHNA UNIVERSITY
Registrar
FARIDABAD

Table of Contents

1 Purpose

The purpose of this Data Management Policy is to protect the electronic data and information belonging to, held or used by, MRU University. It aims to provide a framework within which the roles and responsibilities of those who manage or use the data and information are defined. The intention of the Policy is to enable access to data and information held by MRU, to the greatest extent possible, consistent with legislation and relevant MRU policies, whilst ensuring that electronic data is protected from unauthorized use, access and breaches of privacy.

2 Definitions

2.1 Data

"Data" means information in a form which can be processed and is a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information.

2.2 Data Controller

"Data Controller" means the organization or body which ultimately controls the content and use of data. Under this policy, the Data Controller means the University, rather than any individual, department, school, college, administrative unit or research unit, as for legal purposes it ultimate owns and controls all Data held by the University.

2.3 Data Owner

"Data Owner" means the most senior person/individual in the department/school/college/ administrative unit/research unit within which the data is created. An exception can be made if this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area. Further explanation of this term is provided below.

2.4 Data Custodian

"Data Custodian" means an individual or department/school/college/administrative unit/ research unit (e.g. IT Services) to which data is entrusted on behalf of the Data Controller for the purposes of storage and/or processing.

2.5 Data User

"Data User" means any person who uses, processes, stores, manipulates data held by the University

2.6 Processing

"Processing" means performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data;
- Collecting, organizing, storing, altering or adapting the data;

- Retrieving, consulting or using the data; e.g. reports generated from centrally held databases
- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, deleting or destroying the data.

2.7 Data Subject

A "data subject" means an individual who is the subject of or identified in the data.

2.8 Personal Data

"Personal data" means data related to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the Data Controller. Personal data would include the age of the individual, their home address, their educational and employment history, information relating to their financial affairs, marital status. Users taking personal data outside of the University need to adhere to the Encryption guidelines, as set out in the Guidelines to encryption standards.

2.9 Staff

"Staff" means all full-time and part-time employees of the University, including staff funded externally but under contract to the University.

2.10 Student

"Students" mean all full-time and part-time registered students of the University.

2.11 External Parties

"External Parties" means all the University's subsidiary companies, contractors, researchers, visitors and/or any other parties who are granted access to the University's IT Resources.

2.12 Sensitive Personal Data

"Sensitive personal data" means personal data relating to:

- The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject.
- The physical or mental health or condition or sexual life of the data subject;
- The commission or alleged commission of any offence by the data subject; or
- Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

3 Scope

This Policy governs any electronic Data held by the University. The Policy has been formulated on the basis of the following principles:

Data generated and/or held by the University are key strategic assets that must be correctly managed and controlled so as to ensure their availability, integrity and confidentiality and to protect the University's resources, reputation, legal position and ability to conduct its business. In addition to its legislative responsibilities, the University values the privacy of the individual and the management of Data must be handled in way that protects that privacy.

4 Data Management Policy

4.1 The Data Controller

It is the data controller's responsibility to ensure that appropriate data management policies are in place so that the data owners can ensure they are compliant with legislation to the best of their ability.

4.2 The Data Owner

Every set of data must have a Data Owner. The Data Owner has overall responsibility for the quality and integrity of the data. Specifically, the Data Owner is responsible for:

- Deciding the criticality and sensitivity of the data and classifying the data accordingly
  Authorizing access to Data
- Authorizing the use of the data, e.g. what processing takes place on the data
- Regularly reviewing access privileges
- Assessing the risks to the data. Risks could include but are not limited to:
  a) Theft
  b) Data Loss – due to lack of proper backups
  c) Neglect – Old hardware being recycled without proper data sanitization
  d) Online File Share
- Data Users and Data Custodians need to be made aware of the potential consequences of data theft or loss so the relevant parties can act so as to mitigate these risks;
- Ensure that appropriate contingency plans are in place to safeguard the data and ensure that they or the Data Custodian have the appropriate backup and disaster recovery plans in place.

The Data Owner is the most senior person in the area within which the data is created unless this role has been explicitly delegated to someone else. In the case of

Functional Area	**Student Data**	**Staff Data**	**Financial data**	**Data warehouse**	**Research Data**
Data Owner	Registrar	HR Director	Accounts	IT Director	Principal Investigator

An inventory will be maintained of all the University's major electronic information assets and the ownership of each asset will be clearly stated. Within the information inventory, each information asset will be classified according to sensitivity and criticality. Sensitivity has three categories: a) Public data

b) Data for Internal Use Only
c) Confidential data (including Personal Data and Sensitive Personal Data)

4.3 The Data Custodian

In many cases data will be entrusted to an individual or a department/school/ college/administrative unit/research unit (e.g. IT Services) for the purposes of storage and/or processing in which case they take on the responsibilities of the Data Custodian. This relationship between owner and custodian is often managed by a contract or service level agreement which clarifies specific responsibilities for each party, typical Data Custodian responsibilities include:

- Maintaining the integrity and confidentiality of the data entrusted to them.
- Ensuring that access to the data is restricted to those individuals authorized by the data owner.
- Ensuring that processes undertaken on the data have been authorized by the data owner.
- Having adequate backup and recovery procedures in place for the data, taking into account the sensitivity and criticality of the data as characterized by the Data Owner.
- Providing any information necessary for the Data Owner to fulfill their responsibilities.

4.4 The Data Users

Anyone using or processing University Data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They must comply with the relevant policies of the University (as may be amended from time to time) and with all applicable legal requirements, particularly in relation to data protection and copyright. The data should only be used for the purposes approved by the data owner.

a) Data Users are responsible for protecting their access privileges – Usernames and Passwords for University Systems should not be shared

b) Data generated from central systems that cannot readily be accessed externally, e.g. DMIS, ITS, and HRIS etc. should not be removed from campus without first seeking permission from the Data Owner. Data from these systems is both personal and sensitive so care should be taken when looking to access the information externally.

c) Users should be especially vigilant in complying with this policy when transferring data to mobile equipment such as laptops, tablet devices, phones, USB memory sticks, PDAs, DVDs etc., as they have a greater risk of being lost or stolen.

   i. Anyone accessing information systems remotely to support the business activities of the University must be authorized to do so by the Data Owner of this data. (Permission can be implied given the fact that the system allows the Data User to log in remotely) The strategic importance and sensitivity of the data being accessed needs to be considered and common sense should be used in these situations.

d) Removal off-site of Confidential Data must be properly authorised by the Data Owner. The potential fallout from the theft or loss of said Confidential Data should be considered by both the Data User and Data Owner before removing the data off-site. If necessary the Data Custodian (e.g. IT Services) can be consulted to ensure all possible safe guards are being used e.g. laptop encryption.

e) Confidential Data or information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout

the transfer. Please refer to UCC's IT Security Policy (link set out in section 4 above) and Guidelines on Encryption link set out in section 4 above), this procedure outlines the encryption standards recommended by IT Services.

f) Unsolicited electronic mail (aka SPAM) should not be acted upon or forwarded, a definition for bulk email can be found in the bulk email procedures. If a Data User fears they may have responded to a SPAM email they should contact the staffithelpdesk@ucc.ie immediately to have their access credentials updated.

g) Email addresses should be checked carefully prior to dispatch to avoid sending information to unintended users.

i. Where the information contains data of a personal nature, extra vigilance is required. While it is acknowledged some users will need to process (including transmit) personal data as part of their job, all Data Users are required to comply with UCC's Data Protection Policy (link set out at section 4 above) when processing personal data. A list of Data Protection guidelines are available online at http://www.ucc.ie/en/it-policies/guidelines/

4.5 Storage Media

Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved. IT Services will advise Data Owners and Data Users as to the appropriate media type.

4.5.1 Disposing of equipment/storage media

When permanently disposing of equipment containing storage media, all Confidential Data and licensed software must be irretrievably deleted before the equipment is moved off-site.

Any third party used for external disposal of the University's obsolete data-bearing equipment must be able to demonstrate compliance with the University's information security policies. Where appropriate and/or where the data being disposed of contains Confidential Data, as categorised by the Data Owner, the third party will enter into a service level agreement which documents the performance expected and the redress available in case of non-compliance and, where it contains personal data, the data protection contractual commitments required to be given to the University by law.

4 Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT department. On receipt of notice (or where the University otherwise becomes aware) of any

suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

5 Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

7 Further Information

If user have any queries in relation to this policy, please contact:
General Manager of IT Services